

The Disabled Accessible Voting Equipment Project

A requirement of the Help America Vote Act

Project Summary Report (January 2007)

www.metrokc.gov/elections



Project Summary Outline

1. Introduction & Major Calendar Milestones
2. Budget
3. Training
4. Community Advisory Committee
5. Education & Outreach
6. Electronic Voting Security
7. Conclusion & 2007 Elections Outlook
8. Appendix
 - Security Plan
 - News reports
 - Guest editorials
 - Protecting elections
 - Front page of AVU webpages



The audio ballot allows individuals with limited vision vote independently and in private by listening to the ballot and then registering their choices on the numeric keypad.



Major Calendar Milestones

Cast Ballot



投票



Over the past 18 months, there have been many highlights on the way to reaching compliance with the Help America Vote Act in King County, WA. The Disabled Accessible Voting Equipment (DAVE) project was appointed to implement the laws requiring every polling location in King County

have at least one voting device that is accessible to voters who are blind or visually impaired (RCW 29A.12.160 and HAVA Section 301 (1)(3)). In 2006 King County had 509 polling places spanning more than 2,700 square miles.

To satisfy these requirements, the DAVE project team selected and implemented a voting system that: 1) is accessible to voters with disabilities; 2) meets state and Federal certification; and 3) serves to benefit all voters in King County with a highly accessible alternative to previous voting methods and/or environments. The DAVE Project followed a path of milestones that eventually led to the 2006 General Election.

In King County, the new voting equipment is dubbed the Accessible Voting Unit, or AVU.

In the primary and general election this fall, more than 21,000 King County voters securely cast their ballot on the new equipment and the state-required audits of the accessible voting unit equipment reflected 100 percent accuracy in a side-by-side comparison of the memory card results and the voter-verified paper audit trail. The successes of the outreach campaign were also of note, as the outreach team connected nearly a million voters. Finally, the project team collaborated with election staff to produce a comprehensive training program and a rigorous revival of poll worker training materials. The following milestones provide an outline of the course of implementation that corresponds to the goals set out in the initial project plan:



Major Calendar Milestones

July	11 - DAVE Project Kickoff
August	25 - Decision on course of action
October	28 - HAVA/DAVE grant awarded
November	8 - Education & Outreach campaign kickoff
December	1 - Community Advisory Committee meeting
January	25 - Community Advisory Committee meeting
February	1 - State Certification of King County's selected AVU 3 - Chinese New Year: Debut of AVU in Chinese-American Community 13 - Purchase Contract signed and completed 17 - Acceptance testing completed
March	3 - Announcement of Call for Art winner: Barbara Scholen
April	5 - Accessible voting webpages launch 6 - Community Advisory Committee Meeting
May	26 - Certification of May Special Election, first deployment of equipment
July	7 - Community Advisory Committee Meeting
August	22 - Bus advertising launch & corresponding earned media campaign
September	25 & 28 - Site visit to Snohomish County 29 - Primary Election certified: over 7,000 AVU votes cast
November	28 - Certification of General Election: over 14,000 AVU votes cast
December	14 - Final Community Advisory Committee

Budget

HAVA Grant Awarded		\$ 4,967,000.00
Council Approved Budget		\$ 4,439,500.00
Purchase contract with Diebold		\$ 1,496,892.27
Project Management Support and Training	\$ 471,496.27	
Equipment (200 units and associated equipment to support the equipment)	\$ 879,352.50	
Software and programming	\$ 42,711.00	
Remaining amount is taxes, shipping	\$ 103,332.50	
Lease contract with Diebold(400 AVU units and associated equipment and 575 Express Poll Units)		\$ 1,266,757.81
Post Production Video Editing Services contract with Modern Digital (Poll Worker Training Video)		\$ 24,900.00
Metro Bus Advertising contract with Titan World Wide		\$ 40,710.00
Consulting Services contract with Forefront Elections (Facilitated Staff Session on HAVA compliance and Accpetance Testing.)		\$ 18,630.00
Project labor and benefits.		\$ 368,820.79
Subtotal		\$ 3,216,710.87
Remaining expendiatures (Facilities lease, printing, supplies, travel, remodeling to EDC - wiring and shelving, motor pool rental ect.)		\$ 293,874.76
Total DAVE Project expended and encumbered 12.12.06 (Based from ARMS reports dated 12.12.06 does not include all totals)		\$ 3,510,585.63
Budget remaining from council approved		\$ 928,914.37
HAVA Grant Remaining		\$ 1,456,414.37



Training

The goals of the DAVE project training schedule were two-fold:

1). Prepare staff for AVU implementation with instruction on the operation, maintenance and voter interface of the new accessible voting system as it pertains to their work group; 2). Classify elements and training points, both mechanical and customer service issues, to incorporate into poll worker training.

ELECTIONS STAFF TRAINING

Implementing a new component to a voting system requires that all staff members understands fully how the new system best integrates with their respective work flows. The King County Elections project collaborated with the vendor project manager and managers of the work flow in order to ensure that the needs of individuals and work groups alike were met.

Between October 2005 and November 2006 King County staff took the following courses to support the successful AVU implementation in King County (number of attendees):

DIEBOLD INSTRUCTOR

- Administrative overview (42)
- Elections Distribution Center Supervisor training (6)
- GEMS I (6)
- GEMS II (7)
- Information Technology Manager Overview (1)
- Train the trainers (12)
- Troubleshooter/Help Desk (22)
- Warehouse support (10)

OTHER INSTRUCTORS

- Adobe Audition recording/file management (5)
- Assisting voters with disabilities (14)



Short description of each course:

DIEBOLD INSTRUCTOR

Administrative Overview (1 day course)

Introduction to AVU; system integration; setting up AVU; opening the polls; voting demonstration; EP 2000 card creation; ending elections and summary reports.

Elections Distribution Center Supervisor (4 day course)

Logic & accuracy (L&A) options; maintenance (storage, battery charge, repair); security keys; AVU elections operations; install memory cards; assigning and changing polling locations; opening and closing polls; troubleshooting lab.

GEMS I (4 day course)

Server technology; security applications and procedures; memory cards; system setup; AccuVote (OS); AVU overview; printer module and peripherals; voter access card and other AVU cards; Ballot Station software; programming and troubleshooting.

GEMS II (4 day course)

Election setup options; ballot options and headers; race options and editing; King County geography; creating districts, precincts and splits and generating relationships between each of those; voting centers; importing audio files; pre-election reports; proofing; Logic and Accuracy testing; Election Day reporting.

IT Manager (4 hour course)

GEMS Overview; download memory cards; AVU components (machines, memory cards & encoders); setup and opening the polls; demonstration ballots and features; closing the polls; programming AVU and Express Poll 2000; key card tool & security features; clear key cards and reset election; and troubleshooting lab.

Train the Poll Worker Trainers (4 day course)

Explain all components of King County Election system; introduction to AVU and Express Poll 2000; setup and breakdown of AVU; program voter access cards; discuss legal requirements in polling place; short troubleshooter lab; basic presentation skills; mock polling place; student poll worker presentations; review.



Training

Troubleshooter/Help Desk (4 day course)

Introduction to equipment; setup polls and demonstrate AVU voting; problem solving lab (trainees attempt to 'repair' or diagnose problems that have been arranged by instructor, for example, paper jam).

Warehouse support (4 day course)

Intro to GEMS, AVU & Optical Scan; system integration; Logic and Accuracy testing; sending results; storage and transport of equipment; inventory control; physical security; troubleshooter lab. Express Poll 2000 training: install flash memory cards; power; assign polling location; open polls & create cards; Logic and Accuracy testing options; change location & logout issues.

OTHER INSTRUCTORS

Adobe Audition - Software used to record and manage audio files (4 hour course)

Introduction to required tools; hardware configuration; microphone placement and recording; basic audio techniques; software screen, keyboard and icon setup; recording and managing files; saving options.

Assisting voters with disabilities (1 day course)

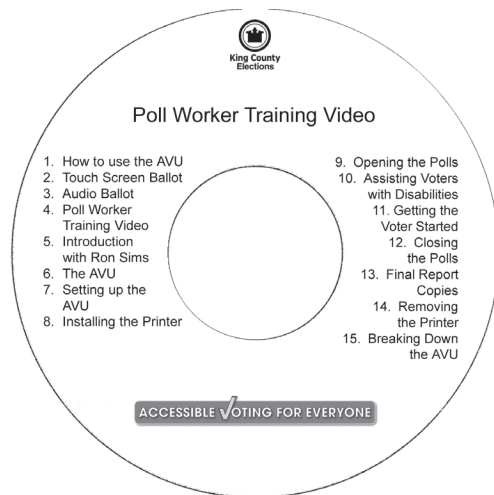
Variation 1: Physical setup of unit; Americans with Disabilities Act requirements; protecting privacy; audio ballot; general tips to increase accessibility; customer service when interacting with voters with specialized needs; explaining the AVU to voters who are blind; disability language & etiquette; short video on assisting voters with disabilities.

Variation 2: Directed and produced video discussing sensitivity issues & Americans with Disabilities Act requirements; polling place operations. Engaged speakers from Office of Civil Rights & Department of Services for the Blind discussed disability etiquette and language; service animals & wheelchair access issues; treating voters as individuals. Speakers from Alliance of People with Disabilities: "people first" messaging; customer service tips (i.e., patience, privacy) for voters with disabilities; demonstrated ballot cast by voter with severe case of Cerebral Palsy.



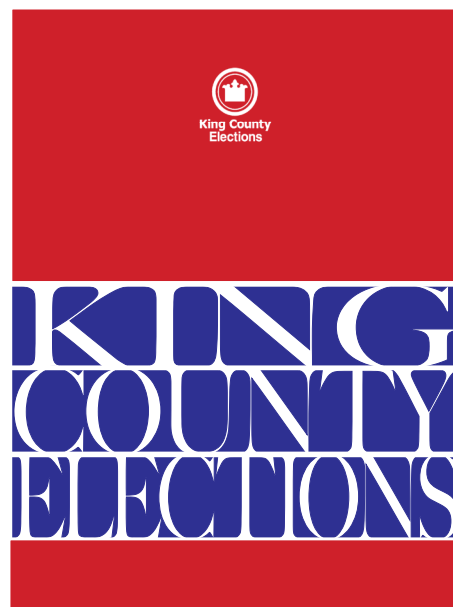
TRAINING SUPPORT MATERIALS

Training video



King County created a new elections judge position to accommodate voters choosing to cast a ballot on the AVU. The AVU judge is solely responsible for a number of things: setting up the unit, opening the polls, encoding voter access cards, closing the polls and preparing the equipment for return. New technology often has a learning curve. To get ahead of that curve, King County produced a training video and sent a copy of the video to all AVU judges and inspectors before the election. To ensure that all judges had the opportunity to view the training video, several viewings were scheduled. Total time: 17.5 minutes.

Updated Poll Worker Guidebook



Adding a new component, the AVU, to the voting systems in King County influenced an extensive poll worker guidebook overhaul. The new look involved content changes as well as format upgrades, and is now edited with Adobe InDesign, professional layout software. The new, 110-page guide to Election Day now includes a Table of Contents page (with page numbers), an easy-to-use index, and more than 20 pages of appendices and glossary notes and hundreds of photos and diagrams.



Community Advisory Committee

King County's innovative approach to implementing the new AVU required by buy-in from a diverse community advisory committee. Washington State later mandated that all counties create a community advisory group to help steer elections administrative decisions on behalf of the disability community. The Community Advisory Committee has met regularly over the past year to discuss the implementation of the accessible voting unit and to advise King County Elections how to best meet the needs of voters with disabilities.



From left to right: Lisa Ivey (King County Elections Intern), Karen Ozmun (King County Office of Civil Rights), Debbie Cook (University of Washington Assistive Technology), Robert Blumenfeld (Alliance for People with disAbilities), Meghann Seiler (King County Elections Intern), Larry Verhei (Governor's Committee on Disability Issues and Employment), Bonnie Duncan (King County Fiscal Specialist), Linda Johnson (League of Women Voters), Debbie Siah (Section 203 Coalition), Gurine Nordby (King County Democrats), Bill Huennekens (King County Elections).

Missing from photo: David Lord (Washington Protection and Advocacy Systems); Jeanette Murphy (Alliance for People with disAbilities); Toby Nixon (WA State Representative); Monica Tracey (King County Republicans); Kris Lawrence (National Federation of the Blind, Greater Seattle Chapter); Cynthia Brothers (Section 203 Coalition).

Education & Outreach

King County Elections followed a communications plan established in February 2006 in an effort to communicate with staff, the County Executive, and the public. The objectives of the campaign were three-fold: educate voters about the implementation of the AVU; register voters and educate the public with new information; recruit [tech-savvy] poll workers to operate the AVUs on Election Day. In total, the education and outreach campaign reached more than one million audience members during the course of the year.



To begin, King County Elections held a series of focus groups and meetings with the community advisory committee to determine the topics, themes and proper disability etiquette to incorporate in our outreach messages. In January of 2006, the campaign kicked off at a meeting of the Greater Seattle Chapter of the National Federation of the Blind.

PHASE I

The communication strategy directed the campaign to begin by networking through the disability community to prepare those voters with disabilities for the implementation of accessible voting units and learn how to design our outreach material in the most accessible way. The goal was to have all voters who might benefit from the new voting system to know about the equipment, and to have an opportunity to cast a demonstration ballot before Election Day. Significant importance was placed on the practice vote, specifically to enhance the confidence level with new technology and equipment.

The community advisory committee engaged local contacts within the disability community and often arranged meetings or events themselves. Committee members and community leaders enlisted to act as stakeholders and consulted with the project team on how to contact hard-to-reach populations. This provided the project an invaluable foundation from which to network throughout the county, for instance the Washington Talking Book and Braille Library; Evergreen Reading Radio (for individuals who are blind); Department of Services for the Blind.

PHASE II

After the initial series of presentations to voters with disabilities, the project turned to a wider audience to include civic services groups, Republican and Democratic Party gatherings,



Education & Outreach

minority and other community association meetings. We found that the Phase I outreach events were essential in networking into Phase II, and furthered the project's goal to get the message to all types of groups of voters.

PHASE III

In order to maximize coverage of the county, the DAVE project hired three interns to join the outreach team. All three interns were political science majors at the University of Washington. With the new recruits, we broadened the audience levels to include public events, festivals and fairs, for instance, the King County Fair and a public service announcement on KOMO Television's Northwest Afternoon. One weekend in late July, the outreach team was present at all of the top three entertainment picks, according to NWSource.com: a popular social events calendar maintained by the Seattle Times: the Capitol Hill Block Party, the Ballard Seafood and Sidewalk Festival, and the Seafair Torchlight Parade.



Charlie Kinder of Seattle, who is blind, cast a demonstration ballot in November of 2005. Since then, Charlie has been a proponent of accessible voting in King County and an avid spokesperson for King County Elections.

Outreach Materials

BUS ADVERTISING

Phase III also included a bus ad campaign during the course of the fall elections, that included with one or more interior advertisements on every bus. Under Section 203 of the National Voting Rights Act (1965), King County is required to provide all election materials in Chinese for the sizable Chinese-American community here.

A blue bus advertisement with a background image of the Statue of Liberty and the Washington State Capitol. The text is in white and yellow. It reads: "ACCESSIBLE VOTING FOR EVERYONE" in large white letters. Below it, "For thousands of voters with disabilities, Independence Day is September 19." in white. At the bottom, "For information about accessible voting in the Primary, call 206-296-VOTE." in yellow. The King County Elections logo is in the bottom left.

ACCESSIBLE VOTING FOR EVERYONE

For thousands of voters with disabilities,
Independence Day is September 19.

For information about accessible voting in the Primary, call 206-296-VOTE.

Exterior English Bus Ad – 60 advertisements (24" x 88" or 24" x 65")

A blue bus advertisement with a background image of the Statue of Liberty and the Washington State Capitol. It features a white icon of a person with a cane on the left. The text is in white and yellow. It reads: "ACCESSIBLE VOTING FOR EVERYONE" in large white letters. Below it, "Accessible voting equipment is available at the polls" in white. A bulleted list follows: "• Easy to read, larger and high contrast ballot text", "• Audio ballot options available in English and Chinese", and "• Tactile pieces available to assist blind voters". At the bottom, "For more information about accessible voting, call 206-296-VOTE" in yellow. The King County Elections logo is in the bottom right.

ACCESSIBLE VOTING FOR EVERYONE

Accessible voting equipment is available at the polls

- Easy to read, larger and high contrast ballot text
- Audio ballot options available in English and Chinese
- Tactile pieces available to assist blind voters

For more information about accessible voting, call 206-296-VOTE

Interior English Bus Ad – 1000 advertisements (11"x17")

A blue bus advertisement with a background image of the Statue of Liberty and the Washington State Capitol. The text is in white and yellow. It reads: "ACCESSIBLE VOTING FOR EVERYONE" in large white letters, followed by "方便投票機，人人可用" in white. Below it, "For thousands of voters with disabilities, Independence Day is September 19." in white. To the right, in Chinese: "對數以千計體能有障的選民，九月十九乃獨立自主日。". At the bottom, "For information about accessible voting in the Primary, call 206-296-VOTE." in yellow, followed by "有關初選方便投票的資訊，請致電 206-296-1544." in yellow. The King County Elections logo is in the bottom left.

ACCESSIBLE VOTING FOR EVERYONE
方便投票機，人人可用

For thousands of voters with disabilities,
Independence Day is September 19.

對數以千計體能有障的選民，
九月十九乃獨立自主日。

For information about accessible voting in the Primary, call 206-296-VOTE. 有關初選方便投票的資訊，請致電 206-296-1544。

Interior Chinese Bus Ad – 250 advertisements (11"x17")

A blue bus advertisement with a background image of the Statue of Liberty and the Washington State Capitol. The text is in white and yellow. It reads: "ACCESSIBLE VOTING FOR EVERYONE" in large white letters, followed by "方便投票機，人人可用" in white. Below it, "For thousands of voters with disabilities, Independence Day is September 19." in white. To the right, in Chinese: "對數以千計體能有障的選民，九月十九乃獨立自主日。". At the bottom, "For information about accessible voting in the Primary, call 206-296-VOTE." in yellow, followed by "有關初選方便投票的資訊，請致電 206-296-1544." in yellow. The King County Elections logo is in the bottom left.

ACCESSIBLE VOTING FOR EVERYONE
方便投票機，人人可用

For thousands of voters with disabilities,
Independence Day is September 19.

對數以千計體能有障的選民，
九月十九乃獨立自主日。

For information about accessible voting in the Primary, call 206-296-VOTE. 有關初選方便投票的資訊，請致電 206-296-1544。

Interior Chinese Bus Ad – 250 advertisements (11"x17")

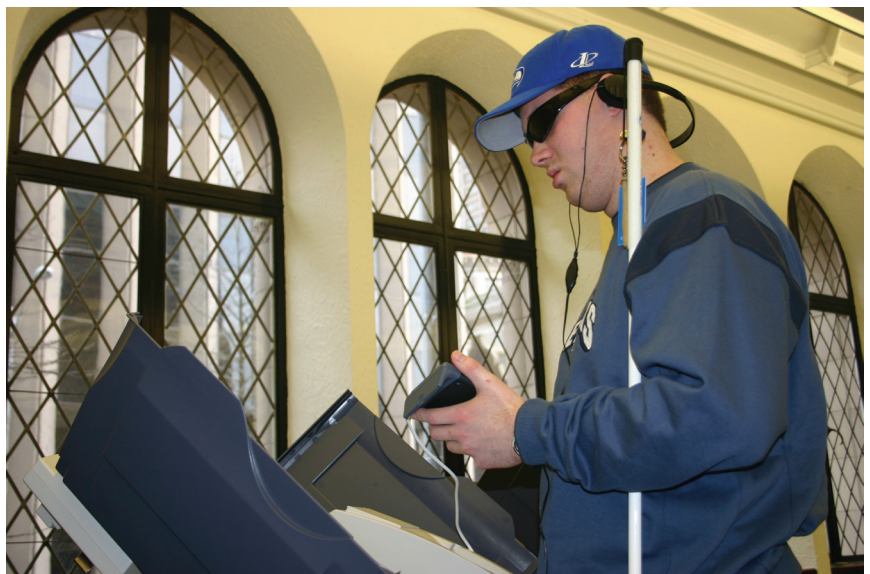


Outreach Materials

WEB SITE

The main elections website (www.metrokc.gov) offers a link to “Accessible voting at the polls” (with English and Chinese versions). The accessible voting homepage provides learning tools, information and support materials for voters to access at their leisure. Information is provided using multimedia and in plain text form, making it user-friendly for voters with assistive technology, such as JAWS readers.

- Accessible voting homepage
- Chinese homepage
- Instructions
 - o Instruction booklet
 - o Demonstration ballot (Flash)
 - o How to vote video (2 minutes)
 - o How to vote an audio ballot (plain text)
- Demonstration ballot (Requires Macromedia Flash 7.0 or greater; 3 minutes)
- Frequently asked questions
 - o Learn how to operate the numerical keypad
- *Protecting elections in King County* (PDF)
 - o (This is the King County Elections response to the Brennan Center Report, an electronic voting security memorandum from NYU Law School)
- Community Advisory Committee
- Community Outreach events
- Glossary of terms
- Poll worker application
- Contact us



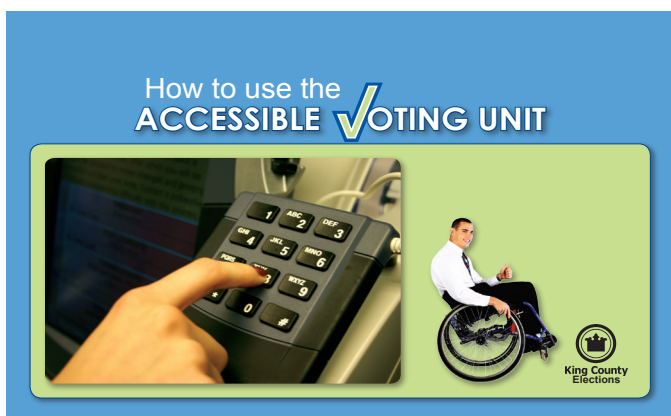
Jacob Struiksma casts an audio ballot at a demonstration with the Greater Seattle Chapter of the National Federation for the Blind



Outreach Materials

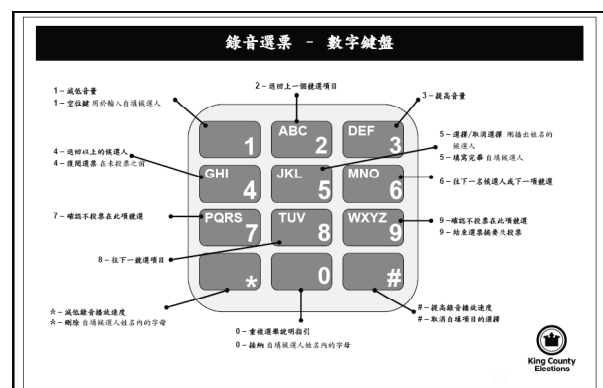
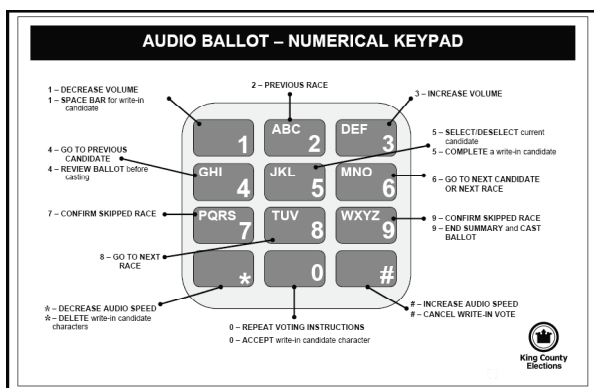
EASY-TO-USE INSTRUCTIONAL CHART FOR POLL VOTERS

The flip chart is a handy-sized 5"x7"booklet and was produced as a quick "How-to" for voters. Only 13 pages long, the flip chart is printed in full color on card stock with a matte laminate for ease-of-use. These booklets were used at events to give a voter an overview of how the AVU provides increased accessibility at the polls with two types of ballots and various balloting options. The flip chart is bilingual and is available at every polling place to aid voters in understanding how the new system works.



NUMERIC KEYPAD - QUICK REFERENCE GUIDE

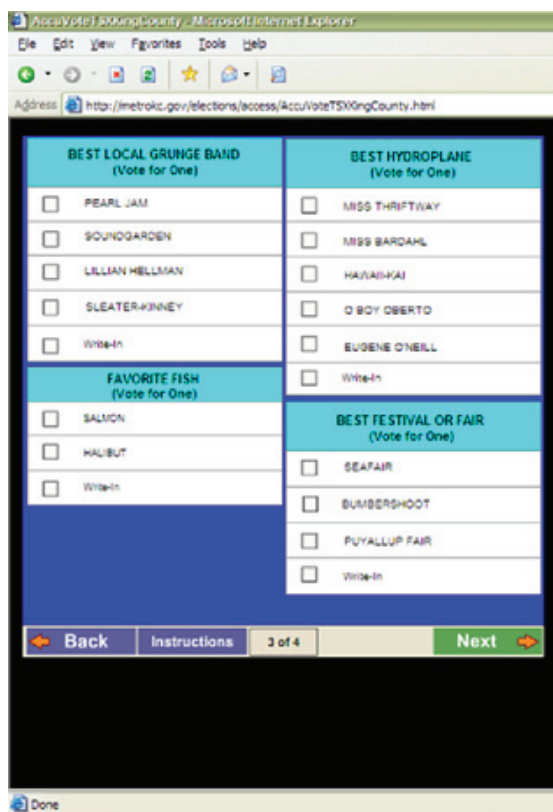
The audio ballot allows voters with visual limitations to vote independently and in private. The keypad quick reference guide displays the numerical keypad in an 11" x 17" large text format. The guide defines each number as to how it is used to register choices in the races and measures on the ballot. The guide was also transcribed into Braille; every polling place had a large text English, large text Chinese and Braille version for voters to reference before casting an audio ballot.



Outreach Materials

INTERACTIVE DEMONSTRATION BALLOT ON THE WEB

Produced in collaboration with the vendor, the web demonstration ballot offers voters with Internet access the choice to practice using the new voting system before they go to the polls. Voters were able to use the mouse to point-and-click their way through a demonstration ballot. Races on the demonstration ballot included “Best of King County” races, such as “Best Dog Park,” and “Best Skiing Area.”



VIDEO: HOW TO USE THE ACCESSIBLE VOTING UNIT

A 2.5 minute video was produced in-house and narrated by local KING 5 Television Meteorologist Jeff Renner. The video teaches the viewer about the availability of the AVU at the polling place, the touch screen and audio ballots and the accessible options offered by the new system.

Outreach Events

Date of Event	Partner/Name of Event	Number of Attendees
25-Oct-05	DAVE Project Kick-off Demonstration for Elections Staff	25
8-Nov-05	General Election Day Demo (<i>three locations</i>)	75
21-Nov-05	Focus Group I	12
30-Nov-05	Focus Group II	12
12-Dec-05	Connections Group	5
13-Dec-05	Focus Group III	11
30-Dec-05	Focus Group IV	12
3-Jan-06	VSAW information and referral	3
21-Jan-06	National Federation of the Blind, Greater Seattle Chapter	28
3-Feb-06	Chinese New Year Luncheon	200
7-Feb-06	Election Day Demonstration, Shoreline Senior Center	100
17-Feb-06	Lighthouse for the Blind Awards Ceremony	30
22-Feb-06	Department of Services for the Blind, Orientation class	30
17-Mar-06	State School for the Blind Board of Directors	12
24-Mar-06	OSOS College Civics, Ellensburg, WA	45
29-Mar-06	Evergreen Reading Radio Interview (<i>WTBBL</i>)	5,000
1-Apr-06	Poll Worker Recruitment, Democratic Party, Renton	40
21-Apr-06	Students of Color Conference, SeaTac	250
26-Apr-06	College Civics Week, UW	35
29-Apr-06	Bellevue Square, voter registration	150
29-Apr-06	WCCD Annual Meeting, Seattle Center	75
30-Apr-06	OCA Meeting, Mercer Island	55
3-Jun-06	Walk for Rice, Seward Park	750
10-Jun-06	Seattle Newcomer's Event, Seattle Center	375
17-Jun-06	Juneteenth Celebration	450
20-Jun-06	National Camps for the Blind	45
21-Jun-07	Ellensburg Employment Conference	250
24-Jun-06	South King Council of the Blind & United Blind of Seattle Picnic	60
8-Jul-06	International District Summer Festival	2,500
11-Jul-06	FamilyWorks Fremont Food Bank	40
13-Jul-06	Kent Cornucopia Days	6,000
15-Jul-06	Alliance of People with Disabilities Picnic	30
19-Jul-06	King County Fair	8,500
26-Jul-06	West Seattle Senior Center	9
28-Jul-06	Capitol Hill Block Party	9,000
29-Jul-06	King County Advocacy Fair	60
29-Jul-06	SEAFair Torchlight Parade	300,000



Outreach Events, cont.

Date of Event	Partner/Name of Event	Number of Attendees
30-Jul-06	Ballard Seafood Festival	50,000
9-Aug-06	Issaquah Rotary	40
10-Aug-06	Highland Community Center	25
11-Aug-06	Washington Council for the Blind Statewide Meeting	20
12-Aug-06	South King Council of the Blind Meeting	10
12-Aug-06	Republican Picnic	1,500
14-Aug-06	Seattle Indian Health Board	12
16-Aug-06	Multiple Sclerosis Association BBQ	50
17-Aug-06	Family Resource Center Food Bank- Redmond	5
19-Aug-06	Pasefika Pacific Islander Festival	2,500
23-Aug-06	Seattle Indian Health Board Elders	25
23-Aug-06	Aging and Disability Services Legislative Forum	200
24-Aug-06	Renton Rotary	25
28-Aug-06	North Bellevue Senior Center	40
29-Aug-06	Merrill Gardens (Senior Center)	18
30-Aug-06	Public Service Announcement on <i>Northwest Afternoon</i>	500,000
1-Sep-06	Maple Valley Community Center BBQ	40
2-Sep-06	Bumbershoot	100,000
6-Sep-06	Seattle Public Library LEAP	15
6-Sep-06	Rotary Club of Auburn	40
7-Sep-06	VSA Vision Gallery First Thursday Art Walk	60
7-Sep-06	King County Unincorporated Area Councils	80
8-Sep-06	Auburn Senior Center 5th Anniversary Celebration	100
9-Sep-06	Legislative Luncheon for National Federation of the Blind WA	40
9-Sep-06	KIXI Grandparents Day Fair	250
11-Sep-06	South Seattle Senior Center	30
11-Sep-06	Renton City Council Meeting (<i>televised</i>)	5,000
12-Sep-06	Redmond Family Resource Center Multi-Agency Staff Presentation	10
12-Sep-06	Northaven Community Center	25
15-Sep-06	Enumclaw Senior Center	10
18-Sep-06	Community Services for the Blind and Partially Sighted	20
21-Sep-07	Developmental Disabilities Residential Conference	300
22-Sep-06	Rainier Rotary Club	30
25-Sep-06	Executive Director of the Deaf-Blind Service Center	3



Outreach Events, cont.

Date of Event	Partner/Name of Event	Number of Attendees
26-Sep-06	Northaven Community Center	30
27-Sep-06	South Seattle Community College	100
4-Oct-06	Green River Community College	150
5-Oct-06	Alliance of People with disAbilities Candidates Forum	100
7-Oct-06	Issaquah Salmon Days with OSOS (Website number: 150,000; estimated visibility in the 10,000 range)	10,000
9-Oct-06	Cleveland High School	140
11-Oct-06	The Center School	45
11-Oct-06	Evergreen Reading Radio Interview (<i>WTBBL</i>)	5,000
13-Oct-06	STAR Center	13
13-Oct-06	University District Rotary	60
17-Oct-06	Roosevelt High School	120
18-Oct-06	Auburn Kiwanis Club	35
18-Oct-06	Renton Senior Group at Highland Community Church	50
19-Oct-06	Four Freedoms Senior Center	30
23-Oct-06	Horizon House	30
26-Oct-06	Sammamish Rotary Club	45
26-Oct-06	Garfield High School	160
2-Nov-06	Radio Interview with Tony B (<i>Clearchannel</i>)	30,000
Total number of audience:		1,040,805

LEGEND	
	Asian community
	Voters 18-30 yrs
	Voters with disabilities
	Diverse community
	Senior citizens
	Other



Electronic Voting Security

Security is the top priority of King County Elections.

Unfortunately, the vendor has self-incurred a poor public perception and in the past 3 to 5 years the integrity of the election system has been challenged by a variety of individuals and groups. In most cases, there is a genuine interest in the integrity, security and accessibility of the election system, although in some cases, the individuals or groups have only added disorder and confusion to the circumstances. King County Elections sought, therefore, to engage and collaborate with those who had a sincere interest in improving elections in this jurisdiction. King County Elections provided accurate and timely information to the media and stakeholders in order to counter any misinformation disseminated by those whose only intent was to denigrate the integrity of the system.

King County Elections believes that enhancing the accessibility to the voting process should not require a trade-off with upholding the security of the election system. From this philosophy, we developed a three-pronged approach to ensure the accuracy and integrity of the election system in King County with the addition of the accessible voting units.

First, the new equipment was integrated into the existing security system which relies on a number of interrelated processes, systems, and policies that complement and build on each other (see fig. 1 on next page). It was imperative that the new equipment maintained the same tested layers of security that counter inappropriate influence or behavior with the elections system.

External stakeholders, such as the media, party observers, elections oversight groups, the Office of the Secretary of State and the public, provide transparency integral to the detection of potential security issues. Physical and personnel security measures ensure that only authorized individuals are allowed access to critical election spaces, materials, technical systems and ballots. Election staff and volunteers are trained in elections processes and procedures. Those processes are then audited and reviewed for accuracy at multiple checkpoints. Consequently, if one or more layers are defeated, bypassed or proven ineffective, the security and integrity of the election process is still preserved .

Second, the approach included rigorous research into the lessons learned and best practices from other jurisdictions. King County Elections utilized current institutional research conducted to verify that decision-making was founded upon the best and most up to date information possible. One example of this aspect of the approach is the utilization of work done by the Brennan Center for

Justice at the New York University Law School. In a report entitled “The Machinery of

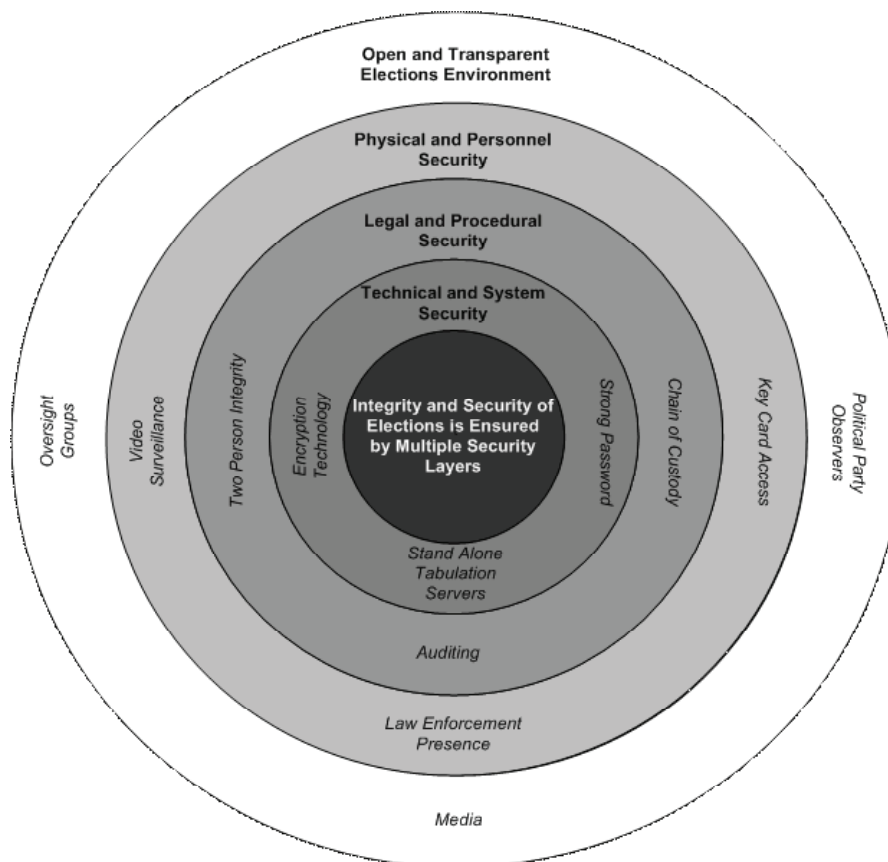


Electronic Voting Security

Democracy: Protecting Elections in an Electronic World,” the center made six recommendations. King County Elections responded to those six important security references with the document, “Protecting Elections in King County.” To respond to these recommendations, King County Elections documented how the Brennan Center’s recommendations were followed and outlined additional security measures; the final document is posted on the Elections website for the general public. See Appendix XXX for the full response.

Finally, the third part of the approach was to include information on our security measures and practices in phases II and III of our outreach and education campaign. During every outreach presentation or demonstration given, a portion of time was dedicated to outlining the security measures and the specifics of security features in the new equipment. Further, interns and election personnel trained on the details and concepts of security for the new equipment staffed booths at fairs and festivals to maximize the public’s exposure to the security features of the accessible voting equipment.

Layers of Election Security



Conclusion & 2007 Elections Outlook

The DAVE project team accomplished the project objectives set out in the initial project plan. The project team implemented specific requirements from both the Help America Vote Act and Washington State Election law in a quality and successful manner. All post-election audits, a state law, resulted in 100 percent accuracy. Additionally, the implementation was duly aligned with the mission statements and strategic technology goals of Records, Elections and Licensing Services and the Department of Executive Services. Related business processes have encountered similar successes.

Beginning with the May 16, 2006 special election, King County Elections has had a voting system in place that:

1. Provides required functionality;
2. Provides the necessary accessibility for voters with disabilities;
3. Is certified for use in Washington State;
4. The selected vendor provides long-term financial viability and is a leading elections solution provider.

In order to act as responsible stewards of County and Federal grant dollars, the DAVE project team designed the implementation of the designated system based on extensive research of best practices in other US counties, and through discussions with outside consulting agencies, committees and other third parties.

Finally, the success of the implementation hinged, in part, on the success of the education and outreach campaign. With the Community Advisory Committee underpinning the communication network, King County Elections engaged the voting public and disabilities community in an education and outreach campaign. The DAVE project provided comprehensive training for staff and poll workers, with a concentration on increasing the awareness of disability etiquette and proper terminology.

In terms of public outreach, a conservative count finds that the outreach campaign addressed over a million audience members over the course of eight months. Tangible results and effective community outreach was accomplished through the abilities of three college interns hired as the outreach and education team.



Conclusion & 2007 Elections Outlook

Lessons Learned

Three key lessons were learned over the course of the AVU implementation. First, the success of the project can be attributed to implementing the AVU in a small, special election prior to a large, county-wide election. Planning and project start dates should be scheduled with an appropriate time allowance for adequate planning, research and outreach to the community.

Second, a strong education and outreach campaign effort was integral to the successful implementation of the project. This includes staff and poll worker training, and the corresponding materials updated to assist with success of the implementation.

Lastly, it is important to have close engagement and communication with non-project members of the staff that are helping to complete project objectives. Adding to this final point, more communicating should be done between Elections Staff and the special projects unit (DAVE) regarding the project, specifically how the project affects each member and work groups after the project team is dissolved.

2007 Elections Outlook

While the 2006 elections cycle successfully incorporated the new system, there will be ongoing issues for operations and maintenance of the AVU. It will be important to maintain awareness and progress regarding the public perception of the security of electronic voting. Similarly, poll worker training on the equipment and training support materials must be in order to maintain effective equipment operations.

Recommendations

Improving accessibility was a top priority of the DAVE project and King County Elections. Several suggestions exist that should be mentioned as future objectives in regard to the AVU:

Recommendations to be addressed by King County Elections:

- Conduct testing regarding the compatibility of various accessibility accessories, including neck loops (assisting voters who are deaf), and attaching a string to the voter access cards to improve accessibility for voters with limited dexterity;
- Follow up with the suggestion to require audio files of proper candidate name pronunciation on CD.



Conclusion & 2007 Elections Outlook

Recommendations to be addressed by the vendor:

- Wider legs of the AVU for more accessible wheelchair access;
- More options for height and width on the AVU;
- Make the AVU capable of Braille output;
- Begin all screen text in large print;
- Extend the idle time requirement on the AVU;
- Ability to track party preference ballots cast;
- Sip and puff device (assistive technology) certification.

Recommendations to be addressed at the state level:

- Modify English text for greater reading accessibility. The current English language used is of a high level, rendering it inaccessible to voters with low reading proficiency.



Appendix - Earned Media

Publish Date	Headline	Source	Placem ent	Tone	Value	Impressions
17-Oct-06	<i>Can you help?</i>	Seattle Times	High	Positive	\$2,023.68	212,691
20-Sep-06	<i>King County reports minor problems, slow tabulating</i>	Seattle Times	Middle	Neutral	\$13,153.92	212,691
7-Sep-06	<i>Demonstrations teach disabled to use new voting units</i>	King County Journal	High	Positive	\$3,420.00	39,109
4-Sep-06	<i>Look for KC local voters' pamphlet, absentee ballots in the mail</i>	Northwest News	High	Positive	\$1,152.00	16,000
29-Aug-06	<i>New voting units</i>	Seattle Times	Middle	Positive	\$3,035.52	212,691
28-Aug-06	<i>Voting booths give disabled privacy</i>	Seattle Post-Intelligencer	Middle	Neutral	\$14,165.76	126,225
28-Aug-06	<i>Disabled, blind voters get better poll access in primary</i>	King County Journal	Top	Positive	\$2,508.00	39,109
23-Aug-06	<i>Poll workers still needed</i>	Seattle Times	Middle	Positive	\$2,023.68	212,691
23-Aug-06	<i>Accessible voting unit here for primary</i>	West Seattle Herald/White Center News	Middle	Positive	\$928.80	11,000
Total Earned Media:					\$42,411.36	

King County Elections worked closely with reporters and other media outlets to disseminate information to voters. Above is a listing of print media covering the DAVE Project outreach and education campaign and the AVU implementation.



Appendix - Earned Media



SEARCH

Home delivery
Contact us

RSS

[Traffic](#) | [Weather](#) | [Your account](#)

[Movies](#) | [Restaurants](#) | [Today's events](#)

Editorials & Opinion: Thursday, September 21, 2006

[E-mail article](#) [Print view](#)

Guest columnist

A strong vote for ballot access

By Debbie Cook

Special to The Times



This fall, for the first time in my life, I am doing something most Americans take for granted. By using a new electronic voting machine that helps people with disabilities, I am voting on my own, and indicating my preferences for who should run things in my area how, without relying on someone to translate or convey my preferences for me.

This simple yet transformative activity is the result of years of effort by many people (some disabled like me, some not) who have been actively involved in our state's implementation of the Help America Vote Act (HAVA) on behalf of voters with disabilities.



own,
and
effort

Like most voters, we want fair elections and the opportunity to vote independently and have that process work well — not just the equipment, but the whole process, from casting the **ballot** to having it counted accurately.

The driving forces behind the Help America Vote Act were, in fact, issues around voter intent in elections. There have been frustrations, mistakes and questions about voter intent that delayed and cast doubt on election results in recent years and led to long-delayed action on this issue.

Despite that, as I vote this fall, these will be the most fair elections that I have ever voted in. I have never had the right to vote an independent **ballot** before now and had no way of knowing that my vote was ever cast accurately, until now.

The new voting equipment makes this possible. As an information-technology professional and person with disabilities, I am extremely excited about the positive impact this will have on voting **access** in our state.

So, when people debate the validity of the whole election process, remember that an independent **ballot** — something that most voters take for granted — is something that many Americans with disabilities have not had at all.

With that said, this is not an effort to politicize the issue of accessibility. By far, accessibility is not the only issue at hand here. In considering election equipment in our own state, for example, we must comply with the federal HAVA standards, and with rigorous state regulatory standards and local acceptance testing in each county to ensure the integrity and accuracy of each device. The voting systems must also meet the federal requirements for disability **access**.



Appendix - Earned Media

A strong vote for ballot access (cont.)

By Debbie Cook
Special to The Times

In Washington state, we have even gone a step further than many states to ensure accuracy and clarity of voter intent by adding the voter-verified paper audit trail to the system. Finally, if individuals do not want to vote by casting a **ballot** on the electronic machines, there are alternatives to that system available in our state. Again, all of these tools are positively transforming the way voters of all ages and abilities participate in our democracy.

There are people who do not want the new electronic voting equipment implemented. They say it's because the machines do not provide **access** for all people with disabilities and cite some good examples. It's probably worth noting, though, that most of those who object to implementing the equipment are not people with disabilities.

Most of us with disabilities know that accessibility improves over time as the requirements are implemented and expanded. In this case, the manufacturers are addressing federal accessibility requirements, so it is difficult to add additional requirements at the state or local level.

But we can advocate that additional federal requirements be added over time, which will further increase **access** to voting for more people with disabilities. I, for one, looked forward to casting my first independently cast **ballot** on Tuesday.

Debbie Cook is director of the Washington Assistive Technology Alliance and a consultant on technology-accessibility issues for the Washington State Department of Services for the Blind.

Copyright © 2006 The Seattle Times Company



Appendix - Earned Media

Commentary

OPINION

Tuesday, November 7, 2006

Secret ballot available to more voters

KRISTINA LAWRENCE
GUEST COLUMNIST

Twenty-six years ago the Americans with Disabilities Act of 1990 was the first piece of legislation to break down barriers to employment, building access, transportation and services. These legal guarantees are important but don't change the fact that, until this year, having a disability didn't guarantee the right to cast a secret ballot.

As a person who has been blind for 22 years, I've relied on family members and friends to accurately complete my ballot and make my voice heard on important issues, such as funding for schools and public transportation. In 2004, Washington residents like myself learned how important voting was, with just 129 votes separating the top two candidates in the closest gubernatorial race in U.S. history.

It wasn't until this past September during the primary that I, for the first time, truly cast a secret ballot -- my own ballot. It was the first time that I, as an American citizen and voter, felt the privilege of voting and knowing that my vote was truly private.

The Help America Vote Act, which requires one accessible voting unit or electronic voting machine at every polling place across the country, takes accessibility for everyone beyond the Americans with Disabilities Act. For the first time in history, voters who are blind will be able to cast their vote privately with the use of new audio ballots. And for the first time, voters with limited hand dexterity can use a touch screen to cast a ballot independently.

Citing security concerns, local and national critics counseled against implementing the Help America Vote Act. To me, forbidding access to voting in the name of security is to say that it is impossible to have a secure and accessible election. I do not feel the two ideals are mutually exclusive.

Security procedures, poll worker training and audits serve as safeguards for accessible voting equipment.

- Each accessible voting unit in Washington is equipped with a voter-verifiable paper audit trail that prints a paper copy of your ballot choices to confirm your choices before casting your ballot. The paper record of your vote is securely stored and only accessed for an audit or recount.
- Only King County Elections has access to program equipment used for voting and counting ballots and memory cards are programmed and sealed before Election Day to prevent tampering.
- Accessible voting units in King County have no wireless components. The units are not networked to each other, nor are they connected to the Internet or an intranet. Procedures in place ensure the accessible voting units are completely isolated throughout Election Day.
- And finally, the day after the election, 4 percent of all machines deployed on Election Day will be selected at random by political party observers and thoroughly audited in the presence of observers and the public. Official election staff will compare the electronic and paper tally of ballots.

As a member of King County Elections' community advisory board, and a voter who is blind, I applaud the efforts my elections department has made to protect my private vote. With strict procedures in place, rigorous poll worker training and post-Election Day audits, I'm confident that when I go to the polls today my vote will be secure and counted.

Kristina Lawrence of Seattle is the president of the National Federation of the Blind of Washington, Seattle chapter.



Appendix - AVU Web Page



King County

Home

News

Services

Comments

Search

Elections

Records, Elections and Licensing Services Division
Department of Executive Services

ACCESSIBLE VOTING FOR EVERYONE

King County voters with disabilities now have the option of casting a truly secret ballot using an accessible voting unit. Federal law requires one accessible voting unit in every polling place in 2006.

Poll voters will have the option of casting their vote on a paper ballot or an accessible voting unit.



Accessible Voting Information

- [Accessible voting homepage](#)
- [Chinese homepage](#)
- [Instructions](#)
- [Demonstration ballot](#) (Requires Macromedia Flash 7.0 or greater)
- [FAQs](#)
- [Protecting elections in King County](#) (PDF, 44 KB)
- [Community Advisory Committee](#)
- [Community Outreach](#)
- [Glossary of terms](#)
- [Poll worker application](#)
- [Contact us](#)
- [More election information >>>](#)

News

- [Alliance of people with disabilities newsletter](#)
- [Audits confirm accuracy of new accessible voting units](#)

Updated: May 3, 2006

[King County](#) | [Elections](#) | [News](#) | [Services](#) | [Comments](#) | [Search](#)

Links to external sites do not constitute endorsements by King County.
By visiting this and other King County web pages,
you expressly agree to be bound by terms and conditions of the site.

[The Details](#)



Appendix - Protecting Elections



**King County
Elections**

Protecting Elections in King County

In the summer of 2006, the Brennan Center (*New York University Law School*) released an analysis of the security vulnerabilities in direct recording electronic (with and without a voter verified paper audit trail) and precinct count optical scan voting equipment. King County uses precinct count optical scan equipment to tabulate paper ballots at the polls and direct recording electronic equipment to provide accessibility to individuals with disabilities. The following six security recommendations were made in the Brennan Center report, "The Machinery of Democracy: Protecting Elections in an Electronic World," and are followed by King County Elections' response and action taken in an effort to ensure open, transparent and accurate elections.

Read the report online at <http://www.brennancenter.org/>.

Brennan Center Recommendation #1

Conduct automatic routine audit of paper records.

Washington State law requires every accessible voting machine contain a voter verified paper audit trail (VVPAT). This VVPAT will be kept in a secure location and will only be opened by King County election officials for auditing purposes or in the event of a recount. Washington State law requires that 4 percent of all machines deployed in a jurisdiction be audited, regardless whether or not a ballot was cast. The audited machines are selected by political party observers in a random and transparent manner. In the fall 2006 election cycle, of the 508 machines deployed at the polls, 21 will be manually audited.

The audit includes comparing the electronic and manual tally of all ballots cast on the machine.

Chain of custody procedures are also in place to ensure the physical security of the VVPAT. Poll workers are trained in these practices and use the same security procedures used for voted and unvoted ballots.

Brennan Center Recommendation #2

Conduct parallel testing.

King County is currently in discussions with the Office of the Secretary of State regarding options for parallel testing. With the requirement for the VVPAT, the parallel testing requirements in the Washington Administrative Code were removed.



Brennan Center Recommendation #3**Ban wireless components on all voting machines.**

The Brennan Center warns against the presence of wireless channels. Accessible voting units in King County have no wireless components. The units are not networked to each other, nor are they ever connected to either the Internet or an intranet. The King County Elections procedures in place ensure the accessible voting units are completely isolated throughout Election Day. In addition, King County will not modem in results from poll vote counting equipment which includes both accessible voting units and AccuVote machines which tally paper ballots. Instead, results will be manually uploaded to enhance security.

Brennan Center Recommendation #4**Mandate transparent and random selection in auditing procedures.**

Accessible voting machines selected for audit are drawn randomly by lot and by political party observers in a transparent and objective manner. The entire auditing process and all auditing procedures are open to the public and observed by political party observers. Random and transparent audits are done to catch fraud or mistakes in the vote totals. The audit performed in the May 2006 special election resulted in a perfect match between the electronic and paper vote totals.

Brennan Recommendation #5**Ensure decentralized programming and voting system administration.**

Members of King County Elections' staff are responsible for ballot layout and the programming for all elections administered in King County. The ballot layout and programming takes place in county elections offices, in rooms under camera surveillance with controlled and tracked access. The "live election database" used for cumulating results and certifying the election is created by and under control of King County elections staff at all times.

Brennan Center Recommendation #6:**Implement effective procedures for addressing evidence of fraud or error.**

In the event of the evidence of fraud or a malfunction, Washington State Law requires that a report detailing the facts and circumstances be made to the county canvassing board. The canvassing board will then make a determination based on the laws and regulations of the state on how to appropriately resolve the situation. (See RCW 29A.60.210)

Additional King County Voting System Security Measures

A voting system must pass three levels of tests before it can be used in Washington:

1. Federal Qualification Tests;
2. State Certification Tests;
3. Local Acceptance Tests.



King County Elections is restricted in using voting systems, equipment and software that has been certified through the Washington's Secretary of State's Office. Currently four vendors are certified for use in Washington State. Washington State law adds the further requirement that equipment must be certified at the federal level. Once the equipment is certified by State and Federal agencies, King County Elections conducts further quality checks through strict procedural acceptance testing of voting equipment.

Stand-alone server technology

- The computer servers hosting the ballot tabulation, building program and associated components used by King County stand-alone and are not connected to an intranet or the Internet. The servers are stored in locked cabinets in secure access controlled rooms and/or cages. Logging into the servers and ballot programming requires dual passwords held by limited individuals within the Elections staff.

HASH-tested software

- To ensure that King County uses the exact same programming code tested and approved by the Independent Testing Authorities, the software components of the tabulating system used in King County are code tested line for line. The software programming code provided to King County by the vendor has been proven to be exactly the same as the programming code deposited in the National Institute of Science and Technology Software Library.

(King County Elections voting systems software has undergone and passed a hash code test. A hash code is a large number computed from the entire string of bits that form the file. The hash code is computed in such a way that if one bit in the file is changed, a completely different hash code is produced. To minimize the possibility that two different files may generate the same hash code, a sufficiently large hash value is computed. Using this method, files from two software codes are "fingerprinted" and those fingerprints are compared. Files that have matching hash values can be discarded from the investigation without further examination; those that do not match the database should be examined further. See www.nist.gov for more info.)

Procedural checks for logic and accuracy

- Prior to every election, King County Elections subjects each accessible voting unit to logic and accuracy testing. That rigorous testing procedurally checks that each machine properly records, counts and tabulates results correctly. A voting machine must pass logic and accuracy testing before it is set for the election, and then the database memory card is sealed in the unit to prevent tampering. An extensive audit trail is maintained of this process including detailed checklists. This legally-required testing is conducted in the presence of political party observers and is open to the public.

Secured ballot storage

- All electronic media storage used in accessible voting units is tracked and accounted for in the same way paper ballots are handled throughout the entire elections process.

Encrypted election-specific codes



- The tabulation system for the accessible voting units utilizes a Key Card Tool encryption program that sets an encrypted code that is required for any voter card, supervisor card or memory card to be used in a device. The code changes prior to each election. This encryption protects against memory and voter access cards from previous elections or from outside the election environment being used in a current election.

Backup memory storage

- The ballot selections made by the voters are stored in three locations: In a printed version on the voter verified paper audit trail; in flash memory within the accessible voting unit tablet; and on an internal memory card stored and sealed within the voting device. The electronic results are encrypted in both the flash memory and on the memory card. In the event of a recount, the paper ballot or VVPAT becomes the official ballot.

Polling place security procedures

Studies of jurisdictions that experienced problems with vote counting equipment share a common theme of inadequate poll worker training and insufficient procedures. King County carefully tracks lessons learned across the nation and has implemented many of these best practices and security standards. In King County, each polling place is staffed by sworn election workers, who have attended mandatory training. There are numerous checks and balances in place, including separation of duties as each voter moves through the polling place:

- On Election Day, a separate judge is dedicated to the accessible voting unit. That judge receives specialized training and maintains control of the machine key. A training video is mailed to every Inspector and AVU judge a week before the election to remind them about important procedures from their training session.
- Before opening the polls, a "zero proof" printout from each voting machine verifies to election judges there are no votes stored on the memory card and that the races are properly coded for the precinct and election. This report is printed twice (one is kept in the security canister for auditing purposes, and one is sent to canvassing), and is signed by three election workers.
- A voter access card is issued only to qualified voters and not issued until proper identification is shown. Only then is a voter access card programmed for the voting machine.
- The voter access cards are programmed as a one-time use only and are collected after voters are finished voting by the AVU judge.
- Each voter is escorted to an accessible voting unit by an AVU Judge.



- Troubleshooters are assigned to regional zones of between 12 and 16 polling places on Election Day and respond to AVU issues such as printer issues or to replenish supplies and troubleshoot problems. This specialized group of 55 people receives 16 hours of mandatory, hands-on training prior to each election.
- A summary report printout from each AVU confirms the total number of ballots cast on each unit. Three copies of this report are printed (one is kept in the security canister for auditing purposes, one is sent to canvassing, and one is posted in a public place). These are again signed by three election workers.





Appendix - Security Plan



**King County
Elections**

**Security Plan
November 16, 2006**



TABLE OF CONTENTS

Introduction	1
Guiding Laws, Policies, and Best Practices	2-3
▪ Open and Transparent Election Environment	7
▪ Physical and Personnel Security	8
-Physical	
-Personnel	
▪ Legal and Procedural Security	11
-RCWs and WACs	
-Ballot & Document Security	
-Accessible Voting Units and Precinct Count Optical Scanning Devices	
-Polling Place Security	
-Signature Verification	
-Post Election Audits	
-Ballot Tabulation System Testing	
-Two Person Rule	
-External Data Storage Mediums	
▪ Technical and System Security	14
-General	
-Network	
-DIMS Specific	
-GEMS Specific	
-Accessible Voting Units and Precinct Count Optical Scanning Device Specific	
Responsibilities	24
Summary	25



INTRODUCTION

Security of the voting process is paramount to ensuring the public's confidence in elections. The King County Elections Section Security Plan is intended to provide a general overview of tasks as well as roles and responsibilities of selected offices and agencies in maintaining the security of the voting process.

In general, elections systems are almost universally composed of two (2) major independent systems that provide functionality for Election Management / Voter Registration and Vote Tabulation. The King County Records, Elections & Licensing Services (REALS) Division employs two such systems. The system used for election management / voter registration is the Data Information Management System (DIMS). The system used to conduct ballot tabulation is the Global Election Management System (GEMS).

The Records, Elections and Licensing Services Division Director has the authority and responsibility to ensure that all employees working in elections are working in a safe environment. In addition, it is crucial that every vote be counted and that the voting process is secure. The Superintendent of Elections or his or her designee is responsible for overall coordination of security concerns during elections. That position will be clearly identified to all employees as the primary point of coordination of security issues.

Effective security does not rely on a single process, feature, or policy. Effective security requires a number of interrelated processes, systems, and policies that complement and build on each other. The systems, process and policies that comprise layers of security for King County Elections are represented in figure 1 on the following page.

These multiple layers of security systems, processes and/or procedures ensure that elections are not inappropriately influenced. External stakeholders such as the media, party observers, Elections oversight groups, the Office of the Secretary of State and the public provide transparency and are integral to the detection of problems with the elections process. The physical and personnel security measures which have been implemented ensure that only authorized individuals are allowed access to critical election spaces, materials, technical systems and ballots. Elections staff and volunteers are trained in elections processes and procedures designed to ensure the security and integrity of the election process. These elections processes are audited and reviewed throughout with many checkpoints for accuracy. This layered approach ensures that if one or even two layers are compromised, bypassed or proven ineffective the security and integrity of the election process is still preserved.

The contents of this Plan are structured to parallel the layers of security shown in figure 1: open and transparent elections environment, physical and personnel security, legal and procedural security, and technical and systems security.

This Plan's focus is on the policies and higher level processes and procedures that are needed to ensure a secure election environment. Detailed processes and procedures that implement these policies will be the subject of specific guidance documents contained in the Election Section's Procedure Document Control Tree (available upon request through the office of the Superintendent of Elections or the REALS Division Director's Office).

Layers of Election Security

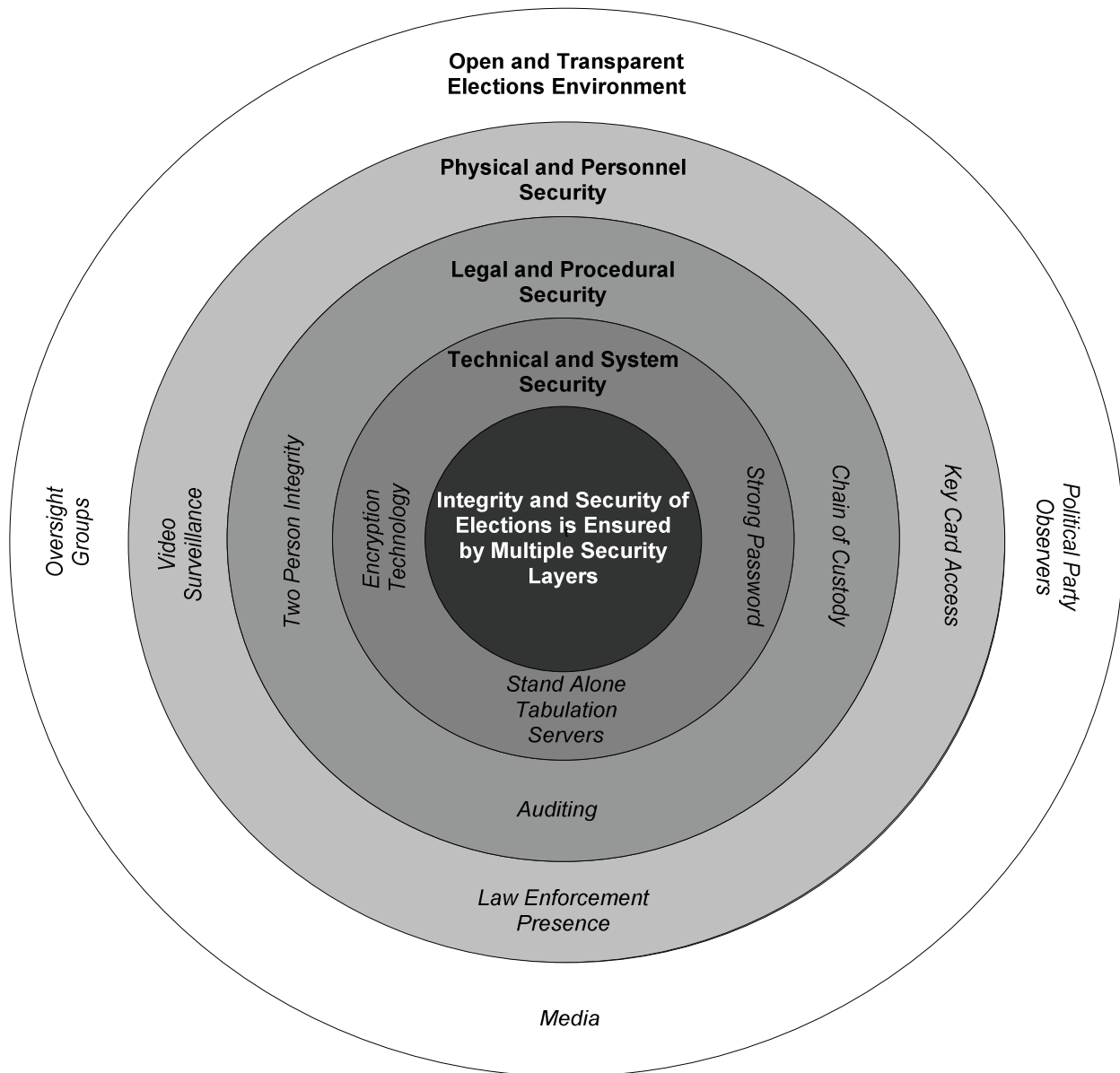


Figure 1



This plan is a dynamic, living document that will be reviewed biennially and updated as significant security issues arise or situations change. After every election, King County Elections staff review the lessons learned from that election and make adjustments to processes, procedures, and systems to improve the effectiveness of operations and security. The King County Elections staff also monitors the experiences of other jurisdictions and scrutinizes studies and reviews by third parties. They then adjust policies and procedures in order to avoid weaknesses experienced or identified by others.

All employees who work in elections or who have a role in elections security share responsibility to ensure that our elections remain secure and that they are conducted with the utmost integrity. To this end, all new employees are required to read and become familiar with this Security Plan as well as any implementation procedures that are relevant to their work areas. All employees will be briefed periodically with the key aspects of this plan. All employees, not just managers, are encouraged to suggest ways to improve the security of the election process. King County Elections also welcomes suggestions from oversight committees and other observers on ways to enhance system security.

GUIDING LAWS, POLICIES & BEST PRACTICES

Laws, policies and best practices that apply to elections include:

- Help America Vote Act of 2002 (HAVA): 42 U.S.C. 15301 to 15545
http://www.eac.gov/law_ext.asp
- RCW Title 29A – Elections <http://apps.leg.wa.gov/rcw/default.aspx?Cite=29A>
- WAC Chapter 434 – Secretary of State
<http://apps.leg.wa.gov/wac/default.aspx?cite=434>
- KCC Title 1, County Council and Elections
- KCC 2.16.035, Department of Executive Services
- Department Policies and Procedures for the Records, Elections and Licensing Services Division, PER 9-2 (DP)
- King County Election Section policies & procedures
- Quick Start Management Guide for Voting System security, U.S. Election Assistance Commission - <http://www.eac.gov/docs/EAC%20Security.pdf>
- Brennan Center report, “The Machinery of Democracy: Protecting Elections in an Electronic World,” –
http://www.brennancenter.org/dynamic/subpages/download_file_36343.pdf

Open and Transparent Election Environment

Administering elections is a monumental responsibility and one in which openness and transparency are essential to gaining and retaining public trust in government. It is the process by which citizens of a democratic republic choose their political leaders, and in the State of Washington, it is a system in which the electorate, through the process of initiative and referenda can directly make law. In any other system or process, it would likely be considered contradictory to require openness and transparency around a set of processes while at the same time restricting access and ensuring strong security, but this is exactly what election administrators across the nation must accomplish. For election administrators, openness and transparency are defined literally, they involve a variety of concepts that combine accountability, transparency, security, and accuracy, to enable access, foster openness, and preserve the integrity of the process. In King County, this is achieved through:

- Building infrastructure design and access
 - Open floor plans, viewing windows, transparent security cage material, and optimized viewing areas are all design elements that facilitate transparency. Additionally, available parking and transit serviced facilities helps minimize barriers that might prevent interested stakeholders from observing various aspects of election processing. King County is also actively planning for the consolidation of all election related activity to occur in a single location. A consolidated elections facility will increase accessibility and benefit openness and transparency.
- Observers/Paid political party observers
 - The requirement for official Observers of the Election Process is grounded in state law. The responsibility for providing the official Observers is with the chair of the county major political party central committees, which he or she may delegate to a Chief Election Observer from the committee staff. Any other Observers are public Observers and are covered under separate policy. It is the responsibility of the Records, Elections and Licensing Services Division Director (Director) to designate the locations where the Observers are to be stationed, and the final approval of the assignment of the Observers.
 - Functions of Observers: Observers serve as a check and balance against ballot fraud by watching to ensure that voted ballots are not changed from the way that they were voted by the voter, that no properly voted ballot is removed from the Election Process without authorization of the County Canvassing Board as provided in RCW 29A.62, nor any other ballot is added to or substituted for the legitimately voted ballots except as provided by law. Each Observer shall also serve to witness the action of the other. This applies to substitute Observers as well when used.
- Documentation of policies and procedures
- Public disclosure of records
- Media access and interest
- Oversight Groups



Physical and Personnel Security

The first line of defense against unauthorized access, tampering with elections results, or other illicit activity is physical and personnel security. If unauthorized individuals cannot get to areas or systems where election activity takes place, they are unable to tamper with or affect the process. Ensuring that Elections personnel do not inappropriately influence or tamper with results starts with selecting highly trustworthy individuals and through additional layers of checks and balances to ensure they do not have the opportunity or inclination to create harm to the process.

Physical

Access Control: Access to the election office and work areas is limited. The physical layouts of the Administration Building and the Election Distribution Center are such that people entering are either recognized or asked to display ID badges. All authorized employees are issued name tags and ID badges and are required to display identification at all times. Staff are issued proximity key cards for opening authorized doors.

In the King County Administration Building (553 Admin), doors are equipped with door position switches that transmit an alarm to the security dispatch center if held open or opened without a valid access card. Duress alarms for protection of staff are located in various locations. Duress alarms are monitored at the security dispatch center 24/7. An alarm condition or duress alarm initiates a camera call-up. King County Employee photos have been loaded into the Access Control System, each card access event calls up the employee picture along with the access granted or denied message at the security dispatch center. Security cameras are located in strategic locations.

Access to the Temporary Election Annex (TEA) facility requires an entry code for the building exterior doors during non-working hours. Keyed suite access is limited to Election supervisors and leads who are assigned keys based on a key plan that limits access to ballot processing spaces to ballot processing supervisors only. All temporary Elections staff, non-Elections county personnel (including building maintenance personnel), and visitors/observers are required to sign in and wear identification badges. Visitors and unofficial observers are required to be escorted through ballot processing space and/or are restricted to observation areas controlled through ropes and stanchions to prevent access to ballot processing staff and election related material.

Polling Locations (approximately 500 locations) - Most polling places do not have hired security in place but will use 9-1-1 to summon local law enforcement officers if a situation arises (specific guidance has been provided to poll workers in the "Emergency Procedures" section of the Poll Worker Guidebook). In a few polling locations, additional security may be hired to maintain the safety of workers and voters.

Election Distribution Center (EDC) Facility - Access to the election work area is limited through personal recognition or display of badges. Uniformed security is present when live voted ballots are on site.

Because of its use in the tabulation of results, GEMS at the Administration Building and the Temporary Elections Annex (TEA) receives extra scrutiny. GEMS tabulation servers are housed in a secured, locked environment, which can only be accessed using key cards by an authorized entrant. This secured, locked room serves as the location where the election database is prepared and where the ballot layout and design quality assurance process is performed. Only authorized elections personnel are permitted to enter the secured server



room unless escorted by an authorized entrant. GEMS server access is given only to key, qualified, and authorized personnel.

Access to the ITS Data Center is controlled by cardkeys and limited to ITS staff. All non-ITS personnel are required to sign in before being admitted and to be escorted by ITS personnel.

Authorization for keycard access to ballot cages and tabulation areas will be granted on an as-needed basis and shall be authorized by either the Director or Assistant Director of REALs or the Superintendent of Elections. All such authorized individuals shall be named on a list and posted at the entry of each cage. Additionally, cage authorized employees shall wear color-coded cage-access credentials.

Uniformed Security Presence: Commissioned police officers in uniform are assigned to the building and provide 24/7 on-site security once voted ballots begin to be processed. During high volume processing, additional officers are assigned to ensure full coverage.

On Election Day, uniformed guards (either off-duty police officers from the City of Seattle, Facilities Management Security Officers or King County Sheriff's Office deputies) are stationed at key points to protect the entry and exit points of elections buildings being used for critical functions. They are present during election ballot counting and transportation of ballots. The security function for various facilities is coordinated between the Assistant Superintendent of Elections Operations, a Facilities Management Division Elections Security Coordinator, and the King County Sheriff's Office Special Operations Section.

Video Surveillance: The Temporary Election Annex (TEA) interior space is monitored by surveillance cameras and motion detection devices on all ballot storage cages and GEMS server locations.

In the King County Administration Building, which houses the administrative offices of the REALs Division, the Elections Operations Unit, the Voter Services group and the Technical Services Group, there are security cameras in multiple key locations.

In the Election Distribution Center (EDC), there is video surveillance of the ballot cages.

All video is recorded 24/7 to a DVR with an archive capacity of 25 to 30 days for post-event review.

Wiring and Data Communications Equipment Closets: These closets are areas of vulnerability where if not properly controlled, could create disruption to communications and data connectivity. All cabling closets will be locked at all times. Keys, combinations, and/or key cards are limited to Elections Technical Services and ITS. Keys are available in sealed key boxes with logs for emergency use if key individuals are not available.

Key Control: All keys to Election spaces are tightly controlled and distributed to individuals with a demonstrable need for access to the space(s) the keys are for. A record of who has been issued a key is maintained. Keys and county identification are collected upon termination. Should a keyed door be compromised through the loss of a key, Elections staff will take immediate action to have the appropriate door (s) re-keyed.

Accessible Voting Units (AVUs) and Optical Scan (OS) Voting Devices: Accessible voting units and precinct count optical scan voting equipment are stored in a secured limited access warehouse facility. Voter access, supervisor, and administrator cards for the AVUs in addition to memory cards for each unit are secured in a locked room with limited access.



The outer case of each of these units is sealed with uniquely numbered, tamper-evident seals. Each of these units, in addition to the associated components are tracked with an electronic inventory system to maintain a documented chain of custody.

These measures enable it to be detected if a unit has been tampered with by either a poll worker during the three days in advance of the election or staff member at any time. By maintaining a documented chain of custody we can detect who may have tampered with a device or when it would likely have occurred.

Pursuant to state law, the accessible voting units create a voter verifiable paper audit trail during the voting process that is securely maintained for the legal retention period. This process is similar to the one used for optical scan paper ballots.

The voter verified paper audit trail is the number one recommendation by critics of electronic voting. This physical security of a voter verified paper audit trail combined with a transparent process, legal, procedural, and technical security measures combine to make a secure and accountable elections system that provides the blind or disabled the ability to cast a secret and independent ballot for the first time.

Servers and Electronic Media:

All sensitive equipment and supplies are secured in locked cabinets, closets and drawers inside the GEMS server room. All computer media and removable data stores like CDs, CD-RWs, diskettes, etc. are locked and secured when not needed. Data backups like CDs and data tapes should be taken off-site to a secure location for disaster recovery.

Locking rack mount cabinets for all GEMS servers have been installed at both the REALS Division administration office (Administration Building) and the Temporary Election Annex site. This security feature deters any attempt at “plugging” into the system, or maliciously trying to shut the system down.

Personnel

Employees, volunteers and observers who work during elections must practice a high level of security. Only authorized personnel with a specific need for access are to be allowed in sensitive areas, including computer equipment rooms, ballot storage areas, and tabulation areas. Others will be accompanied by an escort in sensitive areas at all times.

Upon implementation of this plan and to the extent allowed by law, police background checks will be required for new hires, prior to employment, for personnel who work in areas of heightened security. Heightened security areas will be specified by the Director of REALS in a separate document.

Training about areas of responsibility, sensitivity of information, security of ballots, and chain of custody for the ballots is necessary for all employees and volunteers, and is accomplished through individual work units in training and orientation by work group leads and supervisors.

All personnel and observers are required to wear visible credentials at all times.

A dedicated elections staff recruiter focuses on hiring qualified temporary employees to assist with the various tasks of administering an election. Implementing core skills testing for temporary workers is a significant body of work, but it essentially provides the recruiter with objective information that is used when placing temporary employees into various positions.

Skills and abilities are matched to the positions resulting in greater performance, quality and efficiency. Although hiring temporary workers is dependent on the local job market, the more stringent hiring processes have contributed to an increased attention to detail and adherence to procedures. King County Elections will continue to engage in activities and processes that result in qualified workers being hired.



Legal and Procedural Security

Ballot Programming and Administration: All ballot programming and voting system administration is decentralized in Washington State. King County staff programs and controls these processes in rooms under camera surveillance with controlled and tracked access. All election ballot programming and system administration is performed by qualified King County Election staff. While vendor support personnel are at times on site for advice, they do not perform any actual functions related to the election. This is one of the key recommendations made in the Brennan Center report, "The Machinery of Democracy: Protecting Elections in an Electronic World."

Ballot & Document Security: Voter affidavits are continually being processed in the elections office. When large deliveries of documents arrive they are opened and date stamped. They are then batched for scanning (signature & data capture). Once this process is complete, the batched documents are stored in trays and kept in locked storage cabinets for data entry. When work is being processed in the elections office, it is removed from storage by supervisory staff and assigned to data entry personnel. At the end of each work shift, affidavits & documents are returned to the storage cabinets and locked.

Live ballots, absentee ballots and provisional ballots are handled with an additional level of security. In the elections office absentee ballots are issued over the counter using the Ballot-On-Request module. Ballot stock used to print these in-house ballots is tracked by a stub numbering system and an audit log. Ballot stock remains in locked storage throughout the day and is only accessed when needed. Only authorized elections staff have access to both the ballot stock and the issuing module. This function is assigned only to full time elections staff. These individuals are specially trained to issue and produce ballots using the Ballot-On-Request (BOR) module. At close of business each day, the BOR operators log out of the system. The Superintendent of Elections or a designee is responsible for reviewing the audit logs and coordinating ballot accountability.

All live ballots and ballot stock are secured in the ballot cage area and only authorized personnel have access to this area. While ballots are not actively being processed, the ballot cage remains secured with locks, numbered seals, and ingress/egress is recorded on an access log.

Accessible Voting Units and Precinct Count Optical Scanning Devices: Only federal and state certified voting equipment is used in King County. Prior to deployment all voting equipment is thoroughly acceptance tested using detailed checklists. Prior to acceptance and use, equipment is tested in a mock election and firmware is hash code tested to ensure that programming code delivered by the vendor is the same as that tested and certified by independent laboratories during the federal certification process. A hash code is the result of running data or the object code for an application through a mathematical algorithm. This hash code is unique to that set of data or object code. Changing only one bit of information will result in an entirely different hash code.

In advance of every election all accessible voting units and precinct count optical scan units to be used in the election are tested to ensure that the logic and accuracy of the ballot programming is correct. This legally-required testing is conducted in the presence of political party observers and is open to the public. During this process memory cards containing the election-specific programming (and ballots cast information accumulated on Election Day) are sealed in the units with uniquely numbered tamper evident seals. The unique seal numbers are tracked from the time they are sealed in the warehouse by election staff until the units are returned by poll workers on election night. This enables King County



to detect if the memory card has been disturbed or tampered with during the three days in advance of the election poll workers have the equipment.

Polling Place Security for Accessible Voting Units: Studies of jurisdictions that experienced problems with recent implementations of electronic voting equipment share a common theme of inadequate poll worker training and insufficient procedures. King County Elections carefully tracks lessons learned across the nation and has implemented best practices and security standards. In King County, each polling place is staffed by sworn election workers, who have attended mandatory training. There are numerous checks and balances in place, including separation of duties as each voter moves through the polling place:

- On Election Day, a separate judge is dedicated to the accessible voting units. That judge receives specialized training and maintains control of the machine key. A training video is mailed to every Inspector and AVU judge a week before the election to remind poll workers about important procedures from their training session.
- Before opening the polls, a "zero proof" printout from each voting machine verifies to election judges there are no votes stored on the memory card and that the races are properly coded for the precinct and election. This report is printed twice (one is kept in the security canister for auditing purposes, and one is sent to canvassing), both are signed by three election workers.
- A voter access card is issued only to qualified voters and not issued until proper identification is shown. Only then is a voter access card programmed for the voting machine.
- The voter access cards can only be programmed for one-time use only and are collected after voters are finished voting by the AVU judge.
- Each voter is escorted to an accessible voting unit by an AVU Judge.
- Troubleshooters are assigned to regional zones of between 12 and 16 polling places patrol polling places on Election Day and respond to AVU issues such as printer issues or to replenish supplies and troubleshoot problems. This specialized group of 55 people receive 16 hours of mandatory, hands-on training before each election
- A summary report printout from each AVU confirms the total number of ballots cast on each unit. Three copies of this report are printed (one is kept in the security canister for auditing purposes, one is sent to canvassing, and one is posted in a public place). These are again signed by three election workers.

Post Election Audits: For each primary and general election the REALS Director requests that the political parties select three precincts and a race in each precinct be recounted pursuant to law. This process compares the hand recount of the optical scan ballots and AVU ballots cast in the polling place against the accumulated electronic results.

Prior to certification of each election a random audit of 4% of the accessible voting units deployed in the election is performed. The audit compares a hand recount of the voter verified paper audit trail against the electronic accumulation of results. This is another of the recommendations made in the Brennan Center report, "The Machinery of Democracy: Protecting Elections in an Electronic World."



Ballot Tabulation System and Central Count Equipment Testing: Prior to every election, the GEMS database and central count tabulation equipment are subjected to extensive testing that culminates with the official Logic and Accuracy Test the Friday (four days) before the election. This rigorous testing procedurally checks that the data base and each machine properly records, counts and tabulates results correctly. Each central count device must pass logic and accuracy testing. An extensive audit trail is maintained of this process including detailed checklists. The Logic and Accuracy test of the GEMS database and central count tabulation equipment is conducted in the presence of political party observers and is open to the public. During the primary and general elections, the Office of the Secretary of State is present for the Logic and Accuracy test.

Two Person Rule: To ensure against the possibility of the illegal manipulation of voted ballots, any time voted ballots are not in a sealed container in a secured area during the Election Process, they shall be in the presence of no fewer than two observers who shall not be of the same political party. Ballot processing shall not be curtailed if the requested Observers have not been provided. The Superintendent or Assistant Superintendents may assign pairs of observers at times other than as prescribed above when in his or her opinion, it is warranted.

At any other time ballots in sealed containers are not secured in a vault, they shall be in the presence of at least two Elections Section staff members.

External Data Storage Mediums: Procedures have been created related to the manual handling, storage and disposition of data transfer medium (CD, DVD, disk) for security touch points related to DIMSNeT. These procedures are located in the DIMSNeT Operations and Maintenance Plan, portions of which are available by request through the Superintendent of Election's office or the REALS Division Director's office.



Technical and System Security

The technical security features include the computer security components necessary to ensure data integrity and security of IT and other technical systems, as well as prevent unauthorized access into election systems through the use of best practice tools, processes, procedures, and policies. Proper management of the technical security environment for the system is critical to prevent any unauthorized access to elections systems and data, even if an unauthorized individual has circumvented other layers of security. Technical Security is the last barrier to someone intent on malicious action, though the other layers of security would facilitate detection (e.g. armed Sheriff's deputy security, camera surveillance, and key card access records.)

General

Passwords: Per county IT policy, all systems and users are required to use passwords to log on to workstations, the network and all systems. Passwords must be "strong" passwords. A "strong" password is one that:

- is at least eight characters,
- uses at least three of the following: uppercase letters, lowercase letters, numbers, or special characters (e.g. #, @),
- is not a user's (or user's family) first or last name, birthday, phone number, part of an address, or user's login, and
- can not be found in a dictionary.

County policy requires that network and Windows passwords be changed at least every 90 days. This policy is enforced by Active Directory software. A special password policy for GEMS is discussed in the next paragraph. When changed, a password must be sufficiently different than the last six passwords used. Passwords must never be written down unless they are kept in a locked container. Password must never be shared. Any password that is suspected to have been compromised must be changed immediately. Audit logs should also be checked to determine if anyone inappropriately accessed the system or data and to determine if any malicious modifications were made. Supervisors must immediately notify Technical Services when any employee is released, particularly if they are released under adverse conditions, so that system access can be terminated.

All system and other critical passwords will be written on a piece of paper, folded in half with the writing on the inside, placed in a sealed envelop with the envelop flaps taped with tape that can be written on, initialed across the tape so that the initials from paper across the tape to paper, and the envelope stored in a locked contained in Technical Services. In the event that emergency access is required to a password protected system, permission must be obtained from the Technical Services Manager, Election Superintendent, Assistant Director, or Director. For the tabulation GEMS, the Assistant Superintendent of Ballot Processing and Delivery may also grant permission to open a password envelope. In the event that a password envelope is opened, the password must be changed at the earliest opportunity.

GEMS passwords will be changed based on the election cycle. A new password will be used when an election is initialized, immediately prior to the official Logic and Accuracy (L & A) test, and upon certification of the election. Between the official L & A Test and certification of the election, two-person integrity will be required for access to the GEMS database – that is, the GEMS server password and the GEMS database software will never be known by the same individuals. The server password will be set and known by Ballot Processing and Delivery personnel and the GEMS database password by Technical Services personnel. Before the official L & A Test and after certification of the election, both



passwords may be known by individuals and will normally be limited to Technical Services personnel.

Anti-Virus Software: All King County systems and workstations must have anti-virus software installed (with the exception of GEMS – discussed in the following paragraph). Such software must be set for automatic updates and virus definitions kept up to date. Desktop profiles are set to ensure live updates. Laptop users need to exercise caution to ensure their definitions are maintained.

The tabulation and development GEMS servers are not attached to any external network (Ballot on Request GEMS workstations are). In a closed system, virus infection is extremely unlikely, but it is possible. The potential problem with anti-virus software is that it could affect the GEMS system operation. Diebold Elections Systems Inc. (DESI) has recommended that King County installs and run the anti-virus software during installation of any software and for any updates and then REMOVE the software from the GEMS server. By removing the software, it would remove any potential viruses but also prevent anti-virus software from affecting GEMS operations.

Security patches: The majority of users of Election's systems are using workstations with Windows XP operating systems. All software can have vulnerabilities that allow unauthorized individuals the ability to access systems and potentially access and alter data and modify the systems. This has been particularly true of Microsoft operating systems and applications. As vulnerabilities are discovered, Microsoft (and other vendors) will release security patches. The Information and Telecommunications (ITS) Division evaluates these security patches and determines which patches will be applied to county systems. It is mandatory that any workstations and systems attached to the county network be patched. Generally, this is accomplished automatically by ITS over the network. Users must ensure they leave their workstations powered on when notified by ITS. Laptop users must also ensure that they leave their workstations connected to the network when these updates occur or they must manually ensure the updates are applied if they can't leave the computer attached.

Data backup: It is essential that data be backed up frequently in the event of catastrophic failure to computer or storage systems as well as accidental deletion. In the event data is lost, it can then be restored from the backup. A copy of the backup should also be stored at a second site in the event the primary site suffers damage rendering the backup unusable. For systems connected to the county network, the Information and Telecommunications (ITS) Division provides this service for network disk drives and for servers (e.g. DIMS) they operate on our behalf. Data stored on individual workstations are **NOT** backed up by ITS. It is the responsibility of the user to either back up the data themselves or put a copy of the data on a network drive. ITS does a complete back up once a week and an incremental back up daily. The DIMS System Administrator should request additional complete back ups that coincide with significant events.

GEMS servers are not attached to the network. As a result, ITS does not back up these databases. It is the responsibility of the GEMS systems analyst(s) to perform frequent backups, particularly at critical election events. GEMS backups during tabulation are discussed in the *GEMS specific* section. Specific backups during the development and testing periods are discussed in Election Section Procedures. A copy of the GEMS database as it is at the time the election is certified must be kept for 22 months.

Certification: All software and hardware involved with collecting and tabulating votes must be certified both by the federal government (currently by the Election Assistance Commission) and Washington State Secretary of State. Currently King County uses the



following items that must be certified: GEMS software, AccuVote Optical Scanner and firmware, AccuVote –TSx touch screen hardware and firmware, and Express Poll 2000. Any upgrades to this equipment must also be certified. In addition to state and federal certification, King County Elections will perform acceptance tests on any new or upgraded hardware or software before placing in service.

Hash Codes¹: Before installing or upgrading any software on any system involved with collecting and tabulating votes, King County Elections will verify the software received is the same as that certified through the use of hash code testing.² Procedures for hash code testing are provided in separate documents. In addition to testing software on receipt, King County Elections will work towards periodic hash code testing of a percentage of randomly selected devices for each election to verify that software installed is the certified version and has not been tampered with. For some software (e.g. GEMS application) the software can be tested in place. Other software (e.g. OS scanners) is tested by removing an EPROM from the device and testing it through use of an EPROM reader. Still other software (e.g. AVU) can only be tested by testing the source media (e.g. CD) and re-installing the software on the device. King County Elections is also instituting the practice of hash code testing the GEMS application at the start of each day to prove that the application software is the certified version and hasn't been tampered with. Additionally, the database will be hash code tested at the conclusion of each day's operations and again at the start of the following day's operations to prove that the database had not been tampered with. The database will also be hash code tested upon certification of the election so that any future reporting from the database can be certified to have come from the certified election database. A listing of valid hash codes for certified software can be found at the National Institute of Standards and Technology (NIST) web site - <http://www.nist.gov/vote.html>.

Hash code testing validates that the ballot tabulation software is exactly the same as the software tested and analyzed in the federal and state certification process, and provides election administrators and observers in King County with the assurances needed to be certain that no changes to applications or other critical files have occurred.

Workstation Security: Except for ballot tabulation work, the majority of the work done in elections occurs on desktop workstations connected to networked business applications (e.g. DIMS). As a result, security for systems like DIMS starts with the individual user and the security measures they employ at the workstation level. Thorough security practices and implementation on the servers and networks can be threatened if users don't follow proper security practices at the workstation level. Practices such as leaving their workstations logged on when leaving their workspace or overnight; or writing their password down on their desk blotter can easily provide an unauthorized user access to DIMS defeating the authentication provisions of the database. The more rights the user has in the system, the larger the impact. Users must adhere to the following practices at the workstation level:

- Follow the password policies discussed earlier
- Always lock their computer (or common use computers such as the front desk) when leaving their workstation
- Never give their password to another individual

¹ A hash code is the result of running data or the object code for an application through a mathematical algorithm. This hash code is unique to that set of data or object code. Changing only one bit of information will result in an entirely different hash code. It is similar to an electronic signature.

² All software currently in use has been hash code tested and verified.



- Never install software on their workstations that has not been approved by Technical Services
- Maintain up to date anti-virus definitions and software. Never turn off anti-virus protection
- Do not install any additional hardware unless approved by the Technical Services Manager. In particular, never install any modems or wireless devices.
- All employees are to have read and acknowledged the King County computer acceptable use policy

Laptops: Laptops because of their portability present unique challenges in the security arena. A laptop will frequently be out of areas that are physically secure and in the event of loss or theft leaves information more susceptible to compromise. This unique vulnerability requires additional restrictions. The storage of personal identifying information on a laptop is prohibited unless the information is stored in encrypted format.

No non-county employee laptops are to be connected to the county network. Public Wi-Fi is available in certain buildings throughout King County to enable visitors to access the internet. The public Wi-Fi is not connected to the County's intranet, and access to the county system is protected by the same firewall and other protections identified in the network section below. The county does not provide public Wi-Fi at the Temporary Elections Annex.

Network

Interconnectivity of King County Election's workstations with various election systems servers and connectivity between the different election facilities is accomplished using the county data network. Security of the network is the responsibility of the Office of Information Resource Management (OIRM), Information and Telecommunication Services (ITS) Division. Changes to improve security or rectify problems with existing security arrangements should they arise would be the subject of negotiations between Elections Technical Services and OIRM-ITS.

Architecture³: The transmission of data between the ITS data center and the three (3) Elections locations is carried over I-Net or the KCWAN. The I-Net uses fiber channel leased from a commercial carrier. All switches, routers and other network equipment are King County owned. The KC WAN utilizes King County owned lines. Both the I-Net and the KC WAN are administered by King County ITS. The link to the Elections Distribution Center (EDC) is a 1.5 Mps T1 line. The Administration Building is served by a 100 Mps fiber channel. The Temporary Elections Annex (TEA) is served by a 100Mps link. Both the Administration Building and the TEA use 10/100 Mps lines internally. Routers and switches are in locked wiring and data communication equipment closets to ensure unauthorized individuals cannot get to open ports or areas where they can tamper with the network equipment or configuration.

Connection to the Internet is accomplished through the use of a firewall at the county Data Center. This firewall protects workstations, servers, and systems on the internal network against attacks from the Internet. Measures implemented within the firewall shield IP addresses from the internet reducing the potential for successful malicious activity from external sites. The county also performs anti-virus scanning and intrusion detection at the firewall.

³ Detailed architecture diagrams and specifications are included in a separate document that has restricted distribution.

Servers and software (i.e. GEMS) used for the tabulation of ballots and the reporting of results are not connected to the Internet or to the county's intranet. The local area network for tabulation purposes consists only of tabulation hardware and a local printer. All are physically located in the same space, secured in a separate locked and access-controlled tabulation room or cage.

Election connectivity is via a separate subnet. This provides some measure of protection from problems/attacks affecting other agencies.

Currently, there is no redundant capability for circuits to each building. Any failure of a network link between buildings will leave users unable to connect to the servers until restoration of service. Stipulated response time is 2 hours for switch outages, 12-24 hours for a fiber cut, and 24-48 hours to replace a hub at King Street Station.

Restrictions:

The use of modems on the King County network are prohibited both by ITS and Elections. In the event there is no other way to establish a network connection, the use of a modem must be approved by the Technical Services Manager and the county's Chief Information Officer (CIO). Any use of a modem will only be permitted if there is absolutely no other way to establish communications and will require stringent conditions to ensure adequate security.

Users with legitimate needs to connect to the network from external locations will be provided with Virtual Private Network (VPN) accounts or through a GoToMyPC account. VPNs use tunneling technology with encrypted links to protect the data transmissions. They also use the Active Directory authentication to ensure only authorized users are permitted to connect to the network. GoToMyPC also uses encryption technology and is Internet based using Secure Socket Layer (SSL) not modem based.

There are no wireless devices used within the tabulation system or with any voting device. To prevent any perception of such (through detection of signals with sniffers), wireless technology is prohibited from being used within the ballot tabulation area at the Temporary Election Annex (TEA). Although the county has wireless access points (public _Wi-Fi) at the Administration Building, they are outside the county's firewall and would require a VPN connection to access the internal county data network. Any individual making use of the public Wi-Fi in the Administration Building should be aware that this is an unsecured link and that others may be able to see contents of any transmission. With this in mind, work with data that includes private personal identifying information and other sensitive information will not be conducted unless done over a VPN or through the use of other encrypted links. The use of wireless access points on the Elections subnet portion of the network is prohibited.

Because of the network infrastructure design and safeguards, the use of Active Directory, and other technical best practices, significant barriers exist to help prevent unauthorized access to elections systems and data.

DIMS Specific

DIMS is a fully integrated election management system used to manage voter, jurisdiction, polls & precinct, and contest functions. DIMS does not have any functionality related to vote tabulation or any data related to votes cast. It is the backbone of the majority of functions performed by the King County Elections Section. Failure of this system or inaccurate information would present significant challenges for Election's operations. In addition to the

aforementioned functions, DIMS is a key source of initial (candidate and jurisdiction) information to initialize election preparation in GEMS. Inaccurate or inconsistent information in DIMS would severely impact GEMS ballot preparation. Maintaining a secure and reliable DIMS database and environment is a top priority for the Technical Services Group. Although DIMS security is important, since it does not involve the tabulation of votes, it does not come under the same scrutiny as GEMS does and is not subject to some of the more stringent requirements (such as federal certification). DIMS is also not subject to the same level of security concerns related to the manipulation or destruction of election results since they are not maintained within the DIMS application.

Security for the DIMS applications is a shared responsibility between Election's Technical Services Group and the county's Office of Information Resource Management (OIRM), Information and Telecommunication Services (ITS) Division. As the system owner, Technical Services is responsible for setting the policies and standards for ITS to implement with respect to the DIMS servers (which are housed and operated by ITS). ITS is responsible for the physical security of the servers and the personnel security of administering the servers and interconnecting network. ITS is also independently responsible for the operation and security of the county's internet (I-Net) and Wide Area Network (KC WAN).

King County is also reliant upon the Washington State Office of the Secretary of State (OSOS). OSOS operates the state's Voter Registration Database (VRDB) which is tightly integrated with King County's DIMS. Any lapses or breaches in OSOS's VRDB security could potentially cause good data in DIMS to be overwritten by corrupt data from VRDB. King County Elections monitors the DIMS database, and changes that occur via the VRDB are logged electronically within the DIMS system. Should such a situation occur, King County would work in a coordinated manner with the OSOS to resolve any problems or concerns. The network link is also an additional security touch point that impacts our system.

Architecture⁴: King County Election's DIMS architecture consists of two environments – test and production. The test environment consists of a single server. The production environment consists of an application server for the DIMS application, a SQL server for the database, and an image server. Additional servers that are related to DIMS are the web server and IVR server. All servers except the IVR server are housed in the Information and Telecommunications Services (ITS) Division's Data Center, located on the 24th floor of the Seattle Municipal Tower. King County ITS has the responsibility for the physical security of these servers and the administration of the computer operating system and the SQL database used by DIMS. Users access the system through thin client deployed on individual computer workstations. DIMS users are resident at all three Election locations – Administration Building, Temporary Elections Annex (TEA), and Elections Distribution Center (EDC). Users at all three locations are dependent on the county's data network for access to the server(s).

User Authentication: DIMS maintains its own authentication system that governs not only who can log on, but what rights they have once they have been authenticated. DIMS relies on the Windows password. Within DIMS, users are assigned a user level. This user level governs what subsystems and menus the user has access to and whether they have read only or modification rights. The DIMS administrator maintains user permission tables based on the supervisor's determination of the appropriate access level required to perform their job. DIMS logs all user actions including the end user's login-id, date/time stamp, and data values before and after the change.

⁴ Detailed architecture diagrams and specifications are included in the separate document that has restricted distribution.

SQL Database Access: Permission to the SQL database from DIMS application is obtained through an ODBC connection using Windows Active Directory authentication. The SQL permissions are granted to local groups on the KC domain. Membership to these groups is controlled by Elections Technical Services and administered by the Distributed Computing Systems (DCS) section of ITS.

Installed Software: Internet Information Services (IIS) software is prohibited from being installed on any DIMS server. This closes a potential vulnerability for unauthorized users to access the system.

External Access: Access to Elections' separate subnet will be granted to the DIMS service engineer for database administration and maintenance using the county's VPN network. The DIMS service engineer is required to notify Technical Services whenever they will modification the application and obtain positive consent before making the change.

Business Continuity: The DIMS test server is capable of serving as the DIMS production server in the event of failure. Data is backed up daily (weekly full, daily incremental) providing for restoration of data with a maximum of 24-hour loss.

In the event of an extended loss of KCWAN connectivity to the TEA, the signature verification process would move from that location to the Maynard Room of the Administration Building. Other Elections' procedures provide details on the mechanics of moving operations.

Voter registration data, most of which is considered public information, and the DIMS application, are protected by barriers such as network architecture design, user authentication and use of Active Directory to manage permissions, external access restrictions and protocols, and detailed event logs. These measures, particularly coupled with the other security measures provide a significant level of security and assist in the prevention of unauthorized access or modifications.

GEMS Specific

GEMS is a comprehensive system used to design and build ballots, tabulate central count ballots, accumulate results from polls and early voting (from memory cards), and report election results. GEMS is also used to print ballots for over the counter absentee ballots and provisional ballots.

GEMS is administered by King County Election Technical Services personnel. The Information and Telecommunications Services (ITS) division also provides an analyst to assist in the administration of the system. Authorized users include personnel from Voter Services and Ballot Processing and Delivery units who print ballots. Operation of GEMS for central count processing is shared between Technical Services and Ballot Processing and Delivery.

Architecture⁵: GEMS is installed on only a limited number of workstations/servers. GEMS is installed on two primary servers – one at the Administration Building that is used for development of ballots and testing and the other at the Temporary Elections Annex (TEA) that is used for final testing and tabulation. There is a backup server at each location. Neither of these servers nor their backups are connected to an external network (i.e. outside

⁵ Detailed architecture diagrams and specifications are included in a separate document that has restricted distribution.



the TEA Tabulation Room or the Administration Building GEMS Room) and are prohibited from being so. Any sharing of data files (to the website, Secretary of State, or for other administrative reporting) is done by using portable media, such as CD or diskette. Internal networks exist with each set of servers in the way of printers, AccuVote scanners, and AccuVote TSx Accessible Voting Units (AVU). The use of wireless networking devices on any GEMS server is strictly prohibited. Modem banks that previously existed for electronically reporting results from precincts on election night have been disconnected and will be decommissioned. An external hard drive is connected to the TEA primary GEMS server for data backup purposes.

In addition to these servers, GEMS is also installed on four workstations for specific business purposes:

- Two workstations at the front counter at the Administration Building for Ballot on Request
- A workstation at the TEA for Ballots on Request
- A workstation in the TEA IT office for administrative reporting

GEMS will not be installed on any other computers without the express consent of the Technical Services Manager and the Superintendent of Elections.

Configuration and Implementation: Several restrictions are imposed on the equipment and operation of GEMS servers and workstations. These are necessary to ensure a higher than normal level of security to systems involved in tabulating results or that can produce ballots whose distribution must be control once printed. These restrictions will make unauthorized access more difficult as well as prevent authorized users from taking inappropriate actions that could impair the integrity of the election process.

BIOS: A BIOS password will be assigned on all GEMS servers. Further, the BIOS will be configured to ensure the boot (startup) sequence is restricted to the internal hard drive preventing booting from unauthorized removal media (e.g. CD, floppy diskette, USB device). This will ensure that normal access controls are not bypassed and prevent unauthorized modification of applications and/or data.

Installed software: Software not required to operate GEMS or to enhance security of the system will be installed on the GEMS servers (this restriction does not apply to workstations with GEMS for purposes other than tabulation). This includes GEMS and hash code program. Specifically, Microsoft Office, Microsoft Access, and any other software that enables users to work with Direct Access Objects (DAO) or ActiveX Data Objects (ADO) are strictly prohibited. Although GEMS uses the Jet 4.0 database engine (e.g., Access database engine), MS Access is NOT installed on the GEMS system used for tabulation or ballot development. Activists have pointed to being able to “back door” access to the GEMS database with MS Access application. By not installing (or removing) MS Access, it ensures there is no “back door” on the GEMS tabulation system. Installation of IIS on GEMS servers or workstations hosting GEMS is prohibited.

Use of Access Software: Use of Microsoft Access with GEMS will be limited to a workstation that is used to produce administrative reports⁶. Access is never to be used directly on the GEMS database. The data will be retrieved from the GEMS database through the use of a read-only connection to GEMS from a separate Access application.

⁶ The ability to obtain GEMS data from outside of the GEMS application is necessary because GEMS does not have sufficient reports to meet the various needs of elections administrators, council, and other groups. Since GEMS itself is required to be certified, making quick changes to meet the imposed reporting requirements (either by Diebold or internal staff) is unrealistic.

The GEMS database should always return the same hash code as when it was saved of the tabulation server.

System Configuration: Prior to the official Logic and Accuracy test, the configuration of the tabulation system will be documented in accordance with other Election's procedures. After the L & A Test, the configuration of the tabulation system will not be modified without the express consent of both the Superintendent of Elections and the REALS Division Director. Any approved modifications will be documented on the System Configuration Log, include notification to the Office of the Secretary of State and the King County Canvassing Board. Should such a situation arise, a new Logic and Accuracy test will be conducted according to the established process.

Tabulation Operations: To ensure the security and integrity of tabulated results, several additional steps are taken when ceasing daily operations (including the completion of Logic and Accuracy Tests) and when resuming operations on a subsequent day. A Cards Cast Report will be produced when ceasing operations as well as when resuming operations. The two reports will be reviewed by GEMS administrators and political observers to ensure cards cast when resuming is the same as when operations ceased. Party observers will sign this report attesting to the fact that there was no change. This step will be taken any time there is an interruption in operations such as for lunch, breaks to backup and restore the data base, etc. At the cessation of daily activities, the GEMS database will be backed up to at least three CDs – 2 for storage in the blue bag and one for off-site storage. CDs will be produced in the presence of party observers and will be done to new shrink wrapped CDs. CDs will be sealed and initialed by observers. Before resuming operations on a subsequent day, the database will be restored from a sealed CD rather than using a database resident on the system. Finally, a hash code report will be produced after the back up and again after data is restored. The hash codes will be compared by the GEMS administrators and party observers to ensure no change. Matching hash codes indicates that there was no change in the database⁷.

Audit Logs: Before the Logic and Accuracy Tests, the Window's audit logs for the tabulation server will be cleared. During the tabulation process, these logs will not be cleared. After certification, the logs will be printed and kept with other election records for 22 months.

Business Continuity: As discussed in the architecture section, each primary server is paired with a backup server. In addition, each primary server can serve as a backup to the other. However, since neither server is attached to the network, the database would need to be transported to the other site by removable media (e.g. CD). Application software on the two primary servers is maintained in an identical state. Since the Administration Building primary server is not connected to central count devices, it can serve as a backup to the TEA primary server only in a limited state. In the event of a long term need, additional hardware (if available) could be transported and configured to duplicate the TEA setup. The TEA primary server is fully capable of backing up the Administration Building system with no changes. Alternatively, either server could physically be transported to the other site or even to a third site if necessary for longer term needs.

The TEA GEMS server is served by an uninterruptible power supply (UPS) to facilitate an orderly shutdown and securing of the GEMS database including procedures for Cards Cast Report, hash coding, and backup to CD.

⁷ It is critical that the hash code program be run against the backed up version of the database, NOT the original database. The database is compacted on backup and will yield a different hash code that will not be equal to the hash code of the restored database the next day.

The GEMS tabulation system and tabulation database is the most secured system in use by King County Elections because of its use in tabulating and reporting election results. The hardened physical security measures significantly restrict unauthorized access, and since the tabulation equipment is not networked to any other system, physical access to the server would be required in order to attempt any unauthorized access. Access (i.e. physical access not Access software) logs, log-on credentials, logic and accuracy tests, and hash code testing are all additional measures taken by King County to create a barrier, minimize or eliminate opportunity, and provide for the security and integrity of the tabulation system.

Accessible Voting Units and Precinct Count Optical Scanners Specific

By administrative code, voting units deployed in Washington State are not equipped with wireless technology. Pursuant to state certification requirements memory cards from the accessible voting units and precinct count optical scan units are uploaded directly to the Global Election Management Systems server.

The tabulation system for the accessible voting units utilizes a Key Card Tool encryption program that sets an encrypted code that is required for any voter access, supervisor, administrator or memory card to be used in a device. This code is changed prior to each election by King County Elections staff.

The ballot selections made by the voters on the accessible voting units are stored in three locations: 1) in a printed version on the voter verified paper audit trail, 2) in flash memory within the accessible voting unit tablet, and 3) on an internal memory card stored and secured with a tamper-evident seal within the voting device. The electronic results are encrypted in both the flash memory and on the memory card. In the event of a recount, the paper ballot (or VVPAT) becomes the official ballot.

RESPONSIBILITIES

Elections require participation and responsibility at all levels of government. The list of responsibilities below is not intended to be exhaustive but does provide an overview for various aspects of the elections process.

United States Government

- Provides certification of voting tabulation systems

Washington State Government

- Office of the Secretary of State (OSOS) election review and advisory
- OSOS provides certification of voting tabulation systems
- Updates RCW Title 29A – Elections
- Updates Title 434 WAC – Secretary of State

Cities

- Local security used for jurisdictions with polling locations

King County Government

- Oversees federal, state, and local elections for geographic King County

King County Departments

Department of Executive Services (DES)/Information and Telecommunications Services

DES/Records, Elections and Licensing Services Division (REALS)

- Primary responsibility for overseeing, monitoring and reporting results for elections held in King County
- The verification of absentee ballot signatures
- GIS staff will maintain the geographic boundaries of all major and minor jurisdictions in King County.
- Voter Registration Staff process voter registration affidavits and documents.

DES/Facilities Management Division

- Facilities Security Personnel shall assist the King County Sheriff for security at the King County Administration Building during elections as outlined in Facilities Security Policy and Procedure Manual, Section 5 Special Programs & Assignments, sections 5.95.0 through 5.95.6, July 2003.
- Provide security enhancements for King County owned facilities used for election polling, tabulation and verification activities.

DES/Office of Risk Management

- Polling locations service agreements review

Office of Information and Resource Management (OIRM)

Information and Telecommunications Division

- Supports the Election Management Voter Registration System (DIMS)



- Supports the technical infrastructure required to operate the DIMSNeT software, data and user access through an MOU for 2004 and an SLA agreement for 2005.
- Provides cyber security and cyber assistance

King County Sheriff's Office (KCSO)

- Provide security staffing at King County unincorporated locations and King County owned facilities

King County Prosecuting Attorney's Office

- Provide legal counsel

SUMMARY

Effective security does not rely on a single process, feature, or policy. Effective security requires a number of interrelated processes, systems, and policies that complement and build on each other. The systems, process and policies that comprise layers of security for King County Elections are represented in detail throughout this plan, and illustrated graphically on Page 4, Figure 1.

These multiple layers of security systems, processes and/or procedures ensure that elections are not inappropriately influenced. External stakeholders such as the media, party observers, elections oversight groups, the Office of the Secretary of State, and the public provide transparency and are integral to the detection of problems with the elections process. The physical and personnel security measures which have been implemented ensure that only authorized individuals are allowed access to critical election spaces, materials, technical systems, and ballots. Elections staff and volunteers are trained in elections processes and procedures designed to ensure the security and integrity of the election process. These elections processes are audited and reviewed throughout with many checkpoints for accuracy. This layered approach ensures that if one or even two layers are compromised, bypassed, or proven ineffective, the security and integrity of the election process is still preserved.

This Security Plan details the many safeguards in place that protect elections in King County. Many of these safeguards are not unique to King County Elections, they are deployed throughout election agencies across the state and country. Although many of the safeguards in place today were implemented before they became recognized best practices, or recommendations by outside stakeholders, they are nonetheless based on lessons learned internally, through observation of others, or were existing legal requirements.

The security of elections in King County is also the result of a genuine commitment by election administrators to cooperate with outside stakeholders. Local stakeholder recommendations for improvement have proved beneficial and many have been implemented. The Elections Section continues to be receptive to recommendations made by all interested parties in so much as they positively contribute to election security, election integrity, public trust, openness, transparency, and accountability.



Election administrators and public officials continue to implement and improve safeguards to protect the integrity of elections, as all share responsibility for protecting this process. A key element to improving election security is the participation of voters, state and local officials, political parties and other stakeholders all working in tandem with election officials to identify security threats and areas of opportunity for improvement.

